53-1002145-01
5 August 2011

Brocade Adapters

Troubleshooting Guide

Supporting CNA models 1741, 1020, 1010, 1007
Supporting HBA models 825, 815, 804, 425, 415
Supporting Fabric Adapter model 1860

BROCADE

Copyright © 2011 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCFM, DCX, Fabric OS, FastIron, IronView, NetIron, SAN Health, ServerIron, TurboIron, and Wingspan are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, Extraordinary Networks, MyBrocade, VCS, and VDX are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Brocade, the B-wing symbol, BigIron, DCFM, DCX, Fabric OS, FastIron, IronView, NetIron, SAN Health, ServerIron, TurboIron, and Wingspan are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, Extraordinary Networks, MyBrocade, VCS, and VDX are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://.brocade.com/support/oscd*.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Brocade Adapters Troubleshooting Guide	*53-1001253-01*	New document	June 2009
Brocade Adapters Troubleshooting Guide	*53-1001253-02*	New document	September 2009
Brocade Adapters Troubleshooting Guide	*53-1001253-03*	Updates for Release 2.2	May 2010
Brocade Adapters Troubleshooting Guide	*53-1001582-01*	Updates to support the Brocade 804 adapter	June 2010
Brocade Adapters Troubleshooting Guide	*53-1001253-04*	Updates to support the Brocade 1007 Adapter	September 2010
Brocade Adapters Installation and Reference Manual	*53-1001925-01*	Updates to support Release 2.3	October 2010
Brocade Adapters Installation and Reference Manual	*53-1001925-02*	Updates to support Brocade 1741 adapter	December 2010
Brocade Adapters Installation and Reference Manual	*53-1002145-01*	Updates to support Release 3.0 and Brocade 1860 Adapter	August 2011

Table of Contents

About this Document

In this chapter xi

How this document is organized xi
- Supported adapter hardware and software xii
- Fabric Adapters xii
- CNAs xii
- HBAs xiii
- Fabric OS and switch support xiii
- Host operating system support xiv

Host operating system support for adapter drivers xiv
- Fibre Channel support xiv
- FCoE support xv
- Ethernet support xv
- Hypervisor support xvi

Host operating system support for HCM xvi

What's new in this document xvii

Document conventions xviii
- Text formatting xviii
- Command syntax conventions xviii
- Command examples xviii
- Notes, cautions, and warnings xix
- Key terms xix

Notice to the reader xix

Additional information xx
- Brocade resources xx
- Other industry resources xxi

Providing details for support xxi

Document feedback xxiii

Chapter 1 Introduction to Troubleshooting

In this chapter 1

How to use this manual for troubleshooting 1

Gathering problem information 3

Chapter 2 Isolating Problems

In this chapter 5

How to use this chapter 5

General adapter problems 9
Adapter not reported under server's PCI subsystem. 9
No adapters reported though BCU adapter --list command . . . 10
Port link is not active 10
Device drivers not loading for all adapter instances 11
Installer program does not autorun 12
Host system freezes or crashes 12
Operating system errors (blue screen) 13
Driver event messages appearing in host system log files. . . . 13
BCU version mismatch warning 14
Errors or problems when entering BCU commands 14
bcu pcifn --list and vhba --query commands return errors 14
I/O data traffic issues 15
Support Save file is too large (Windows only) 15
Host system running Microsoft Windows fails to hibernate . . . 16
Driver incompatible with CNA drivers 16
Brocade BCU desktop shortcut missing (Windows only). 16
Driver installation fails and system cannot be booted 17
Cannot remove Linux driver with uninstaller application or scripts 17
Removing Ethernet (network) drivers causes error 17
Files needed for bfad.sys message appears 18
Cannot roll back driver on all adapter instances using Device Manager 18
Device drivers not loading due to lack of MSI-X interrupt vectors 18
Driver installation fails on ESX systems 19
Errors when using GUI-based software installer 19
Errors when installing brocade_driver_linux_<versions>.tar.gz package 19
UEFI boot problems 20
BIOS boot problems 23

Fabric Adapter problems. 27
VLANs and teams persist after changing port to HBA mode . . 27
HCM not discovering all Ethernet ports for vNICs 28

HBA problems 28
No adapters found on local host" message in HCM 28
Quality of Service performance issues. 28
Quality of Service not functioning. 29
Trunking problems 29
Unable to create more than 126 Virtual (NPIV) ports for adapter 30

CNA problems 31
Cannot manage CNAs after attempting upgrade to 3.0 drivers 31
VMQs not created for virtual network adapter instances 31

Network interface problems (CNA or NIC) 32
Ethernet loopback test problems 32
Ethernet link ports or LOM not coming up on reboot in Linux . 33
Loss of adapter hardware address in Linux 33
Loss of adapter IP address in Linux 33
Network stack runs out of heap 34
NIC numbering unexpected on VMware systems 34
Ping to remote host is failing. 34
Receive-side scaling disables unexpectedly 35
Applications using TDI driver stop responding. 36
RSS network throughput decreases 36
SNMP MIB browser not displaying information on VLAN -related OIDs. 36
Teaming errors 36
VLAN creation and operation problems 37
Teaming or VLAN operations through HCM fail 38
Poor network performance 39
Binding issues after Hyper-V enabled with teaming 39
FCoE and Fibre Channel problems 41
Loss of sync and loss of signal errors in port statistics 41
Fabric authentication failures 41
Adapter is not showing in the fabric 41
Virtual devices not listed in name server 42
Adapter not registering with the name server or cannot access storage 42
FCoE link is down 43
I/O problem on connected FCoE device 44
I/Os are not failing over immediately on path failure in MPIO setup 44
Disk I/O requests cause low throughput and high latency on Linux 45
Disk I/O requests cause low throughput and high latency on VMware 45
DCB network problems 45
DCB is not enabled 45
HCM and HCM Agent problems 46
Failed to connect to agent on host... error when using HCM . . 46
HCM Agent service cannot start 49
HCM Agent not auto starting if 3.0 driver updated with 2.3 HCM 49
Unable to completely uninstall HCM. 49
Time on HCM screens does not match system time 50
Verifying Fibre Channel and DCB links (stand-up adapters) 50
Adapter driver installation verification 51
Confirming driver package installation with HCM 52
Confirming driver package installation in Windows systems . . 52
Confirming driver package installation in Linux systems 53
Confirming driver package installation in Solaris systems 54
Confirming driver package installation in VMware systems . . . 54
Troubleshooting mezzanine card problems. 55

Additional references for isolating problems. 56

Chapter 3 Tools for Collecting Data

In this chapter 57
For detailed information 58
Data to provide technical support 58
Data collection using host system commands 59
Data collection using BCU commands and HCM 61
Support Save 61
Using BCU commands 65
Data collection using Fabric OS commands (Brocade switches only) 66
Adapter event messages 67
Logs 69
Host system logs 69
HCM logs 70
Logging levels adjustment. 71
Statistics 73
Authentication statistics 73
DCB statistics (CNA only). 74
DCB query (CNA only) 75
FCoE statistics (CNA) 75
Fabric statistics 76
Displaying FCP initiator mode statistics 77
FCP initiator mode statistics 77
Firmware statistics. 78
I/O performance 79
Logical port statistics. 80
Performance data 81
PHY module statistics 81
Port Performance. 82
Port statistics 82
Real-time and historical performance statistics 83
Remote port statistics 84
Quality of Service statistics (HBA). 85
Trunking attributes. 85
vHBA statistics 86
vNIC statistics (CNA or NIC). 86
Virtual port statistics 87
VLAN statistics for a team (CNA and NIC) 88
VLAN statistics for a port (CNA and NIC) 89

Diagnostics 89
Beaconing (stand-up adapters) 89
Internal and external loopback tests 90
Ethernet port loopback test (CNA) 91
PCI loopback test 92
Memory test 93
Pinging Fibre Channel end points 93
Adapter temperature 94
Queue test 94
SCSI test 95
Trace route 95
Echo test 96
Collecting BIOS data 97
Displaying BIOS data through BCU 97
Display BIOS data through HCM 97
Collecting LLDP data (CNA) 97
Collecting SFP data (stand-up adapters) 98
SFP properties 98
Predictive optical monitoring (POM) 98
Collecting port data 99
Displaying port properties 99
Displaying DCB port properties (CNA) 99
Displaying Ethernet port properties (CNA or NIC) 100
Displaying FCoE port properties (CNA) 100
Displaying FC port properties (HBA) 101
Displaying remote port properties 101
Displaying logical port properties 102
Displaying virtual port properties 102
Displaying the port log 102
Displaying the port list 103
Performing a port query 103
Displaying port speed 103
FCP-IM I/O profiling 104
Enabling FCP-IM profile through HCM 104
Collecting teaming information (CNA or NIC) 104
Displaying team data and statistics through HCM 104
Displaying configured team data through BCU 105
Authentication settings 105
Displaying authentication settings through HCM 105
Displaying authentication settings through BCU 106
PHY module data 106
QoS settings (HBA) 106
Determining QoS settings through HCM 107
Target rate limiting settings (HBA) 107
Determining target rate limiting settings through BCU 107
Determining settings through HCM 108

Persistent binding 108
Displaying Persistent Binding settings through BCU 109
Displaying Persistent Binding settings through HCM 109
Adapter properties 109
CNA Properties 109
HBA Properties 110
Adapter queries 111

Chapter 4 Performance Optimization

In this chapter 113
Tuning storage drivers 113
Linux tuning 113
Solaris tuning 114
Windows tuning 114
VMware tuning 116
Tuning network drivers (CNA or NIC) 116
Windows tuning 116
Linux tuning 117
VMware tuning 117
Solaris tuning 119

Appendix A Adapter BIOS and Event Message Reference

Adapter BIOS messages 121
Adapter driver event messages 122

Appendix B HCM and Installer Message Reference

Index

About this Document

In this chapter

- How this document is organized xi
- Host operating system support for adapter drivers xiv
- Host operating system support for HCM xvi
- What's new in this document xvii
- Document conventions xviii
- Notice to the reader xix
- Additional information xx
- Providing details for support xxi
- Document feedback xxiii

How this document is organized

This manual provides troubleshooting information on Brocade host bus adapters (HBAs), converged network adapters (CNAs), and Fabric Adapters. It is organized to help you find the information that you want as quickly and easily as possible.

The document contains the following components:

- Chapter 1, "Introduction to Troubleshooting" provides an introduction and approach to troubleshooting adapter problems, as well as tips for gathering problem information. A checklist is also provided to verify that required procedures have been followed during installation.
- Chapter 2, "Isolating Problems" provides information on common adapter problems and procedures to diagnose and recover from these problems.
- Chapter 3, "Tools for Collecting Data" provides a summary of diagnostic and monitoring tools available through the Host Connectivity Manager (HCM), Brocade Command Line Utility (BCU), Fabric OS commands, and host system to help you isolate and resolve adapter-related problems.
- Chapter 4, "Performance Optimization" contains guidelines for optimizing adapter performance on your host system.
- Appendix A, "Adapter BIOS and Event Message Reference" contains details on all event messages generated by adapter drivers.
- Appendix B, "HCM and Installer Message Reference" lists all error messages that may display during operation of HCM and the Brocade Adapter Software Installer application. Causes of each message and actions to perform to resolve problems are also included.

NOTE
This publication is a companion guide to be used with the *Brocade Adapters Administrator's Guide*. That publication provides detailed information on adapter monitoring and diagnostic tools in the HCM and the BCU.

Supported adapter hardware and software

This section provides an overview of Brocade adapter supported hardware and software.

Fabric Adapters

Brocade 1860 Fabric Adapter ports can be configured for CNA, NIC, or HBA operation using Brocade Command Utility (BCU) commands. Ports configured in CNA or NIC mode require appropriate 10GbE SFPs or direct-attached copper cables and operate at a 10 Gbps maximum rate. Those configured in HBA mode require appropriate 8 or 16 Gbps Fibre Channel SFPs and operate at an 8 or 16 Gbps maximum rate depending on the installed small form factor pluggable transceiver (SFP+).

Brocade 1860 single or dual-port adapter models can ship in the following configurations:

- Single-port model - 16 Gbps Fibre Channel SFP, 10GbE SFP, or no optics.
- Dual-port model - Two 16 Gbps Fibre Channel, two 10 GbE, or no optics.

Note that although adapters may ship with specific optics installed, you can install any compatible component, such as 8 Gbps FC SFPs, long-wave SFPs, and direct-attached SFP+ copper cables. Refer to the appropriate "Hardware Compatibility" section for the adapter in the *Brocade Adapters Installation and Reference Manual* for more information.

NOTE
Install only Brocade-branded small form factor pluggables (SFPs) in stand-up Fabric Adapters.

CNAs

The following Fibre Channel over Ethernet (FCoE) CNAs are supported:

- Brocade 1007. Dual-port mezzanine CNA with a per-port maximum of 10 Gbps. This is an IBM compact form factor horizontal (CFFh) mezzanine-type adapter that installs on supported server blade.
- Brocade 1010. Single-port stand-up CNA with a per-port maximum of 10 Gbps.
- Brocade 1020. Dual-port stand-up CNA with a per-port maximum of 10 Gbps.
- Brocade 1741. Dual-port mezzanine card CNA with a per-port maximum of 10 Gbps. This is a small-form-factor (SFF) mezzanine card that mounts in a Dell blade server.

NOTE
Install only Brocade-branded small form factor pluggables (SFPs) in stand-up CNAs. Mezzanine CNAs do not have SFPs and external port connectors, but utilize internal ports and connections to switch and I/O modules installed in the blade system enclosure.

HBAs

The following Fibre Channel host bus adapters (HBAs) are supported:

- Brocade 415. Single-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.
- Brocade 425. Dual-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.
- Brocade 804. Dual-port mezzanine HBA with a per-port maximum of 8 Gbps. This HBA installs on Hewlett Packard blade servers.
- Brocade 815. Single-port stand-up HBA with a per-port maximum of 8 Gbps using an 8 Gbps SFP+.
- Brocade 825. Dual-port stand-up HBA with a per-port maximum of 8 Gbps using an 8 Gbps SFP+.

NOTE
Install only Brocade-branded small form factor pluggables (SFPs) in stand-up HBAs. Mezzanine HBAs do not have SFPs and external port connectors, but utilize internal ports and connections to switch and I/O modules installed in the blade system enclosure.

Note the following about HBA support

- This publication only supports the HBA models listed under "HBAs" and does not provide information about the Brocade 410 and 420 Fibre Channel HBAs, also known as the Brocade 400 Fibre Channel HBAs.
- Although you can install an 8 Gbps SFP+ into a Brocade 415 or 425 HBA, only 4 Gbps maximum port speed is possible.

Fabric OS and switch support

Brocade adapters support Brocade Fabric OS and switches.

Fabric Adapters

- Ports on Fabric Adapters configured in CNA mode can connect to Fibre Channel SANs and Ethernet data networks through a compatible FCoE switch. These ports can also connect to an Ethernet data network as a NIC. For a current list of compatible switches, refer to the latest interoperability matrices on the adapters website a www.brocade.com/adapters.
- Ports configured in HBA mode support the Fabric OS and connect to SANs through fabric switches or connect directly to storage. For a current list of compatible switches, refer to the latest interoperability matrices on the adapters website at www.brocade.com/adapters.
- Ports configured in NIC mode fully support the Ethernet protocol and connect directly to the Ethernet LAN.

CNAs

Brocade CNAs must connect to Fibre Channel SANs and Ethernet data networks through a compatible FCoE switch. These ports can also connect to standard Ethernet LAN switch. For a current list of compatible switches, refer to the latest interoperability matrices on the adapters website at www.brocade.com/adapters.

HBAs

Brocade HBAs connect to Fibre Channel SANs through compatible fabric switches or connect directly to storage. For a current list of compatible switches, refer to the latest interoperability matrices on the adapters website at www.brocade.com/adapters.

Host operating system support

Refer to "Host operating system support for adapter drivers" for information on operating systems that support the Brocade Host Connectivity Manager (HCM), Brocade Command Line Utility (BCU), and adapter drivers.

Host operating system support for adapter drivers

This section lists operating system support for all models of the following types of Brocade adapters:

- Fabric Adapters - Refer to the following subsections depending on your port configurations:
  - "FCoE support" on page xv and "Ethernet support" on page xv for ports configured in CNA mode.
  - "Fibre Channel support" on page xiv, for ports configured in HBA mode.
  - "Ethernet support" on page xv for ports configured in NIC mode.
- CNAs- Refer to the following subsections:
  - "FCoE support" on page xv
  - "Ethernet support" on page xv.
- HBAs - Refer to "Fibre Channel support" on page xiv.

NOTE
Specific operating system release levels, service pack levels, and other patch requirements are detailed in the current adapter release notes.

NOTE
Also refer to the latest Brocade interoperability matrices on the Brocade website at www.brocade.com/adapters for a list of supported host systems and operating systems.

Fibre Channel support

The following lists operating systems that support Fibre Channel operation for HBAs and for Fabric Adapter ports configured in HBA mode:

- Windows 2003 R2/SP2 (x86 and x64)
- Windows Server 2008 (Longhorn) (x86 and x64)
- Windows Server 2008 R2/SP1 (x64)
- Microsoft Hyper V for Windows 2008 x86, x64
- Windows 7 (x86 and x64)

- Windows Server Core for Windows 2008 (x86 and x64)
- Microsoft WinPE 3.0 for Windows 2008 (x86 and x64)
- Linux RHEL 4.9, 5.5, 5.6, 6.0, 6.1
- SLES 10 and 11 (x86 and x64)
- Solaris 10 (x86, x64, and SPARC)

NOTE
Solaris is not supported on Brocade 804 or 1007 adapters.

- VMware ESX Server 4.0, 4.1, 5.0 (x64)

NOTE
Drivers and BCU are supported on the VMware ESX platforms. HCM is supported only on the guest system on VMware.

- Oracle Enterprise Linux (OEL) 5.6, 6.0 (x86 and x64), Oracle VM 3.0

FCoE support

The following lists operating systems that support FCoE operation for Brocade CNAs and Fabric Adaptor ports configured in CNA mode:

- Windows Server 2008 (x86 and x64)
- Windows Server 2008 R2/SP1 (x64)
- Microsoft Hyper V for Windows 2008 x86, x64
- Windows 7 (x86 and x64)
- Windows Server Core for Windows 2008 (x86 and x64)
- Microsoft WinPE 3.0 for Windows 2008 (x86 and x64)
- Linux RHEL4.9, 5.5, 5.6, 6.0, 6.1 (x86 and x64)
- Linux SLES 10 and 11(x86 and x64)
- Solaris 10 (x86, x64, and SPARC)

NOTE
Solaris is not supported on Brocade 804 or 1007 adapters.

- VMware ESX Server 4.0, 4.1, 5.0 (x64)

NOTE
Drivers and BCU are supported on the VMware ESX platforms. HCM is supported only on the guest system on VMware.

- Oracle Enterprise Linux (OEL) 5.6, 6.0 (x86 and x64)

Ethernet support

The following lists operating systems that support Ethernet operation for Brocade CNAs and Fabric Adaptor ports configured in CNA or NIC modes:

- Windows Server 2008 (x86 and x64)

- Windows 2008 R2/SP1 (x64)
- Windows Server Core for Windows 2008 (x86 and x64)
- Windows 7 (x86 and x64)
- Microsoft WinPE 3.0 for Windows 2008 (x86 and x64)
- Linux RHEL 4.9, 5.5, 5.6, 6.0, 6.1 (x86 and x64)
- Linux SLES 10 and 11 (x86 and x64)
- Solaris 10 (x86, x64, and SPARC)

NOTE
Solaris is not supported on Brocade 804 or 1007 adapters.

- Xen Hypervisor (x86 and x64)

  Refer to "Hypervisor support" on page xvi.
- VMware ESX Server 4.0, 4.1, and 5.0 (x64)

NOTE
Drivers and BCU are supported on the VMware ESX platforms. HCM is supported only on the guest system on VMware. Network drivers are not supported on IA-64 systems.

- Oracle Enterprise Linux (OEL) 5.6, 6.0 (x86 and x64)

Hypervisor support

The following lists operating systems that support hypervisor operation for Brocade adapters:

- Windows Server 2008 Hyper-V (x64)
- Linux RHEVH 6.x (x64)
- Linux XEN (x86 and x64)
- Linux KVM (x64)
- VMware ESX 4.0, 4.1, and 5.0 (x64)
- Oracle VM 3.0 (x64)
- Citrix XenServer 6.0 (x64)

Host operating system support for HCM

The following operating systems support HCM management for adapters.

- Windows Server 2008 (x86 and x64)
- Windows Server 2008 R2/SP1 (x86 and x64)
- Windows SBS 2011 (x64)
- Windows XP
- Windows Vista
- Windows 7 SP1 (x86 and x64)
- Linux 5.5, 5.6, 6.0, 6.1 (x86 and x64)

NOTE
HCM is a 32-bit application. To use HCM on Linux RHEL 6.0 x64 systems, you must install the x32-compatible libraries because they are not installed by default.

- Linux SLES 10 and 11 (x86 and x64)
- Solaris 11, except Open Solaris (x86, x64, and SPARC)
- VMware ESX Server 4.0, 4.1, 5.0 (x64)

NOTE
HCM is not supported in ESXi systems.

NOTE
HCM is supported only on the guest operating system for VMware.

- Oracle Enterprise Linux (OEL) 5.6, 6.0 (x86 and x64)

NOTE
Specific operating system service patch levels and other patch requirements are detailed in the current release notes for your adapter software version.

What's new in this document

This document adds details on adapter release 3.0 and the Brocade 1860 Fabric Adapter. For further information about new features not covered in this document and documentation updates, refer to the release notes for your adapter software version.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
`code` text	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase.

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
--**option, option**	Command options are printed in bold.
-**argument,** arg	Arguments.
[ ]	Optional element.
variable	Variables are printed in italics. In the help pages, values are underlined or enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, --**show** WWN
|	Boolean. Elements are exclusive. Example: --**show** -**mode** egress | ingress

Command examples

This book describes how to perform configuration tasks using the Fabric OS command line interface and the BCU interface, but does not describe the commands in detail. For complete descriptions of all commands, including syntax, operand description, and sample output, see the *Fabric OS Command Reference* and *Brocade Adapters Administrator's Guide*.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries on MyBrocade. See "Brocade resources" on page xx for instructions on accessing MyBrocade.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Windows, Windows Server 2003, Windows Server 2008, Vista, XP, PE for Windows, Hyper V for Windows, Windows Automated Installation Kit (WAIK), and Windows 7.
Oracle Corporation	Solaris
Red Hat Inc.	Red Hat Enterprise Linux (RHEL)

Corporation	Referenced Trademarks and Products
Novell, Inc.	SUSE Linux Enterprise Server (SLES)
VMware, Inc.	ESX Server
SPARC International, Inc.	SPARC
Hewlett Packard Corp.	BladeSystem
IBM	BladeCenter
Dell	PowerEdge

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

1. Go to the adapters website at www.brocade.com/adapters.
2. Navigate to the adapters **Downloads** page.
3. Select your operating system from the **Downloads** list to display appropriate downloads or download the ISO image.

Brocade resources

To get up-to-the-minute information, go to *http://my.brocade.com* to register at no cost for a user ID and password. A variety of resources for Brocade products is available.

Adapters

For adapter resources, such as product information, software, firmware, and documentation, visit the adapters website at www.brocade.com/adapters.

For additional information on Brocade adapters, refer to the following publications:

- The *Brocade Quick Installation Guide* (provided with your adapter model).
- *Brocade Adapters Troubleshooting Guide*
- *Brocade Adapters Administrator's Guide*
- *CIM Provider for Brocade Adapters Installation Guide*

FCoE Switch

For information on the Brocade FCoE Switch for connecting stand-up CNAs, refer to the following publications:

- *Brocade 8000 Hardware Reference Manual*
- *WebTools Administrator's Guide*
- *EZSwitchSetup Administrator's Guide*
- *Fabric OS Command Reference Manual*

Blade servers and blade system enclosure components

Brocade mezzanine and expansion card adapters are compatible with blade servers, switch modules, interconnect modules, I/O modules, and other components that install in supported blade system enclosures. For compatibility information, visit the compatible blade server and blade system enclosure manufacturer's website. Also refer to the Hardware Compatibility section in Chapter 1 of the *Brocade Adapters Installation and Reference Manual*.

SAN information

White papers, online demonstrations, and data sheets are available through the Brocade website at:

http://www.brocade.com/products-solutions/products/index.page

For additional Brocade documentation, visit the Brocade website:

http://www.brocade.com

Other industry resources

For additional resource information, visit the Technical Committee T11 website. This website provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association website:

http://www.fibrechannel.org

Providing details for support

Contact your Brocade FCoE CNA support supplier for hardware, firmware, and software support, including product repairs and part ordering. Provide the following information:

1. General information:
    - Brocade adapter model number.
    - Host operating system version.
    - Software name and software version, if applicable.
    - syslog message logs
    - **bfa_supportsave** output.

      To expedite your support call, use the bfa_supportsave feature to collect debug information from the driver, internal libraries, and firmware. You can save valuable information to your local file system and send it to support personnel for further investigation. For details on using this feature, refer to "Support Save" on page 61.
    - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions.
    - Description of any troubleshooting steps already performed and the results.

2. Adapter serial number:

   The adapter serial number and corresponding bar code are provided on the serial number label illustrated below. This label is affixed to the adapter card.

   You can also display the serial number through the following HCM dialog boxes and BCU commands:

   - Adapter **Properties** tab in HCM.

     Select an adapter in the device tree, then click the **Properties** tab in the right pane.

   - **BCU adapter –list** command.

     This command lists all adapters in the system and information such as model and serial numbers.

3. Port World-Wide Name (PWWN).

   Determine this through the following resources:

   - Label affixed on adapter card provides the WWPN for each port.
   - Brocade BIOS Configuration Utility.

     Select the appropriate adapter port from the initial configuration utility screen, then select **Adapter Settings** to display the WWNN and PWWN for the port. For details, refer to the Boot Code chapter in the *Brocade Adapters Installation and Reference Manual*.

   - Port **Properties** tab in HCM.

     Select a port for a specific adapter in the device tree, then click the **Properties** tab in the right pane.

   - The following BCU commands:

Command	Function
port –query <port_id>	Displays port information, including the PWWN for the FCoE port. The *port_id* parameter is the port number.
port –list	Lists all the physical ports on the adapter along with their basic attributes, such as the PWWN.

4. Media access control (MAC) addresses. These are applicable to CNAs and Fabric Adapter ports configured in CNA mode only.

   The adapter MAC address can be found in HCM by selecting the adapter in the device tree and clicking the **Properties** tab in the right pane to display the adapter **Properties** panel. Look for the **MAC Address** field.

   Each port has a “burned-in” local port MAC address. This is the source MAC for LLDP communications between the adapter and FCoE switch. To find this MAC address, select a CEE port in the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **Local port MAC** field.

The Ethernet MAC address is used for normal Ethernet operations. To find this MAC address using HCM, select an Ethernet port in the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **Current MAC address** and **Factory MAC address** fields.

Each enode logging in to the fabric through a local adapter port is assigned a MAC address during FCoE Initialization Protocol (FIP) operations. This MAC is assigned for the current FCoE communication only. To find this MAC address, perform one of the following tasks:

- Select an FCoE port in the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **FCoE MAC** field.
- Enter the **port –query** *port_id* BCU command. Look for the FCoE MAC.

NOTE
MAC addresses assigned during FCoE initialization operations cannot be changed using device management applications.

The FCoE Forwarder (FCF) MAC address is the address of the attached FCoE switch. Select an FCoE port in the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **FCF MAC** field.

You can also determine port MAC addresses using the following BCU commands:

Command	Function
port —query *port_id*	Displays port information, including the MAC addresses. The <port_id> parameter is the port number.
port —list	Lists all the physical ports on the adapter along with their Ethernet and FCoE MAC addresses.

NOTE
For details on using HCM and BCU commands, refer to the *Brocade Adapters Administrator's Guide*.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1 Introduction to Troubleshooting

In this chapter

- How to use this manual for troubleshooting 1
- Gathering problem information 3

How to use this manual for troubleshooting

An adapter, such as an HBA, CNA, or Fabric Adapter is one component of a larger network consisting of switches, storage devices, host systems and the cabling and connections to these components. Although there may be a problem in the adapter or an adapter component, the problem could also originate in another network component or connections between components. Before removing and replacing adapters, launching adapter diagnostics, or even gathering statistics on adapter operation, it is important that you perform the following tasks:

1. Fully describe the problem and gather complete information about the symptoms that suggest a problem exists. Refer to "Gathering problem information" on page 3.
2. Isolate or resolve the problem by using information in Chapter 2, "Isolating Problems".

   Adapter problems are organized under the following categories:

   Search through the list of problems in Table 2 on page 5. Problems are organized in the table by problem title, category, and whether the problem is operating-system-specific. Click on a problem to go to the chapter section containing details of possible causes and actions for resolution.

   - "General adapter problems"
   - "HBA problems"
   - "Network interface problems (CNA or NIC)"
   - "FCoE and Fibre Channel problems"
   - "DCB network problems"
   - "HCM and HCM Agent problems"

   Each problem section in Chapter 2 provides a complete description of the problem, possible causes, and actions for resolution. Fixes and actions may reference BCU commands, HCM features, and host operating system commands. These are described in Chapter 3, "Tools for Collecting Data".

   Other helpful sections in Chapter 2 include the following:

   - "Verifying Fibre Channel and DCB links (stand-up adapters)" on page 50.
   - "Adapter driver installation verification" on page 51.
   - "Troubleshooting mezzanine card problems" on page 55.
   - "Additional references for isolating problems" on page 56

3. Use the BCU commands, HCM features, and host operating system commands described in Chapter 3, "Tools for Collecting Data" to gather data for resolving problems.These tools include event logs, operating statistics, and diagnostics.
4. Consider these factors when isolating and resolving the problem:
   - Can the issue be resolved using the latest supported combination of host system BIOS, operating system, operating system updates, or adapter drivers?
   - Refer to "Software installation and driver packages" and "Operating system support" in Chapter 1 of the *Adapters Installation and Reference Manual* for details on driver packages and operating system support. Also download the latest release notes from the Brocade adapters website using the following steps:
     a. Go to the adapters website at www.brocade.com/adapters.
     b. Navigate to the adapters **Downloads** page.
     c. Select your operating system from the **Downloads** list to display appropriate downloads.
     d. Download the release notes from the "Documentation" section.
   - Does the issue persist when the adapter is installed in a different platform or blade server or connected to a different switch port?
   - Does the problem persist if using a different SFP or cable (stand-up adapters)?
   - Can this problem be reproduced on one or more adapters, ports, or host system? Can you identify specific steps that consistently reproduce this problem on one or more hosts?
   - Is the problem documented in release notes for the adapter, operating system, or host system BIOS?
   - Is the problem documented in release notes for the switch and target storage system?
   - Is unexpected behavior intermittent or always present?

   If the problem is in a Fibre Channel or FCoE switch, storage device, or in connectivity between these components, refer to the documentation, help systems, or service providers for that equipment.
5. If you cannot resolve the problem, gather and provide problem information to your adapter support provider for resolution.

NOTE
If troubleshooting information in this manual does not resolve problems, check the installed version of the adapter (chip revision) and driver (firmware version) using the BCU **adapter –query** command. To use this command, refer to "Using BCU commands" on page 65. Also download the latest release notes from the Brocade adapters website at www.brocade.com/adapters and look for known problems relating to the adapter and driver versions. On the adapter website, navigate to the adapters **Downloads** page, and then select your operating system from the **Downloads** list to display appropriate downloads or download the ISO image.

Gathering problem information

Perform the following tasks to obtain as much information as possible before contacting technical support. Be sure to take careful notes for use as a record and reference.

- Describe the symptoms that you are observing. Be specific. Here are some examples:
  - User experiences, such as slow performance or file access.
  - Expected storage devices not visible from the HCM or host system's storage management application.
  - Adapter not recognized by host system BIOS.
  - Adapter not recognized as PCI device by host system operating system.
  - LEDs not functioning on an adapter port that is connected to the fabric (stand-up adapters).
  - All LEDs on adapter port flashing amber (stand-up adapters).
- What happened prior to the observed symptoms?
- Describe all observed behavior that is unexpected and compare against expected behavior.
- Gather information for support:
  - Use appropriate tools on storage targets to gather information such as disk, tape, and controller model and firmware levels.
  - Use the Support Save feature. This feature captures all driver, internal libraries, firmware, and other information needed to diagnose suspected system issues. You can save captured information to the local file system and send it to support personnel for further investigation. For details on using the Support Save feature, refer to "Support Save" on page 61.
- Draw a topology map of the SAN from the adapters to the storage targets. Include the components described in Table 1.

TABLE 1 Topology map details

Component	How to identify
adapter	Model, World-Wide Name (WWN), and driver release level.
Fibre Channel switches	Model, WWN, and Fabric OS version.
Fiber optic links between adapter, switches, and storage ports	Port WWNs connected to all links.
Host hardware	Model and hardware revision.

The **bfa_supportsave** and FOS **supportsave** commands can provide current information for the topology map. Also, consider using the Brocade SAN Health products to provide information on your SAN environment, including an inventory of devices, switches, firmware versions, and SAN fabrics, historical performance data, zoning and switch configurations, and other data. Click the **Services & Support** tab on www.brocade.com for more information on these products.

- Run appropriate diagnostic tools for storage targets.

- Determine what has changed in the SAN. For example, if the SAN functioned without problems before installing the adapter, then the problem is most likely in the adapter installation or configuration, adapter hardware, or adapter driver package. Other examples of things to investigate might be changes in the connected switch or storage system firmware, or an offline switch.

  For stand-up adapters, investigate disconnected or faulty cables between the adapter, switch, or storage controller fiber optic ports. Check if target storage devices are correctly connected to the switch and are turned on.

  For mezzanine or expansion card adapters, make sure that the adapter, the blade server where the adapter is installed, and the modules in the blade system enclosure that support adapter operation are compatible. Verify that the blade server and modules that support adapter operation are installed in the appropriate enclosure bays. Also check whether target storage devices are connected to the appropriate switch, interconnect module, or I/O module in the blade system enclosure and are turned on.
- Record the time and frequency of symptoms and the period of time symptoms have been observed.
- Determine if unexpected behavior is intermittent or always present.
- List steps that have been taken to troubleshoot the problem, including changes attempted to isolate the problem.

Chapter

2

Isolating Problems

In this chapter

- How to use this chapter 5
- General adapter problems 9
- Fabric Adapter problems 27
- HBA problems 28
- CNA problems 31
- Network interface problems (CNA or NIC) 32
- FCoE and Fibre Channel problems 41
- DCB network problems 45
- HCM and HCM Agent problems 46
- Verifying Fibre Channel and DCB links (stand-up adapters) 50
- Adapter driver installation verification 51
- Troubleshooting mezzanine card problems 55
- Additional references for isolating problems 56

How to use this chapter

Operation problems are arranged in this chapter in these categories:

- "General adapter problems"
- "Fabric Adapter problems"
- "HBA problems"
- "Network interface problems (CNA or NIC)"
- "FCoE and Fibre Channel problems"
- "DCB network problems"

Use Table 2 to quickly navigate to sections in this chapter that cover specific adapter problems. Each problem section in this chapter contains a description of the problem, possible causes, and actions for resolution. Click on the problem to link to the appropriate problem section.

TABLE 2 Isolate adapter problems

Problem	Category	OS Specific
"Adapter not reported under server's PCI subsystem"	"General adapter problems"	All
"No adapters reported though BCU adapter --list command"	"General adapter problems"	All
"Port link is not active"	"General adapter problems"	All

TABLE 2 Isolate adapter problems (continued)

Problem	Category	OS Specific
"Host system freezes or crashes"	"General adapter problems"	All
"Operating system errors (blue screen)"	"General adapter problems"	All
"Driver event messages appearing in host system log files"	"General adapter problems"	All
"BCU version mismatch warning"	"General adapter problems"	All
"Errors or problems when entering BCU commands"	"General adapter problems"	All
"bcu pcifn --list and vhba --query commands return errors"	"General adapter problems"	All
"I/O data traffic issues"	"General adapter problems"	All
"Support Save file is too large (Windows only)"	"General adapter problems"	Windows
"Host system running Microsoft Windows fails to hibernate"	"General adapter problems"	Windows
"Driver incompatible with CNA drivers"	"General adapter problems"	Windows 2003
"Brocade BCU desktop shortcut missing (Windows only)"	"General adapter problems"	Windows
"Driver installation fails and system cannot be booted"	"General adapter problems"	Windows 2008
"Device drivers not loading for all adapter instances"	"General adapter problems"	Windows
"Installer program does not autorun"	"General adapter problems"	Windows
"Cannot remove Linux driver with uninstaller application or scripts"	"General adapter problems"	Windows
"Removing Ethernet (network) drivers causes error"	"General adapter problems"	Windows
"Files needed for bfad.sys message appears"	"General adapter problems"	Windows
"Cannot roll back driver on all adapter instances using Device Manager"	"General adapter problems"	Windows
"Driver preinstallation problems"	"General adapter problems"	Windows
"Errors when installing brocade_driver_linux_<versions>.tar.gz package"	"General adapter problems"	Linux
"Device drivers not loading due to lack of MSI-X interrupt vectors"	"General adapter problems"	VMware
"Driver installation fails on ESX systems"	"General adapter problems"	VMware
"Errors when using GUI-based software installer"	"General adapter problems"	All
"System will not boot over SAN or on local disk in Legacy BIOS mode"	"General adapter problems" "UEFI boot problems"	All
"Host not booting from remote LUN"	"General adapter problems" "UEFI boot problems"	All
"Boot devices not available in host's Boot Manager menu"	"General adapter problems" "UEFI boot problems"	All
"Driver and operating system installation failure on boot LUN"	"General adapter problems" "UEFI boot problems"	All

TABLE 2 Isolate adapter problems (continued)

Problem	Category	OS Specific
"Installing Windows 2008 R2 DUD on UEFI system results in offline disk"	"General adapter problems" "UEFI boot problems"	Windows 2008
"Driver and operating system installation failure on boot LUN"	"General adapter problems" "BIOS boot problems"	All
"Target not visible from host"	"General adapter problems" "BIOS boot problems"	Windows
"Ctlr-B option does not display when booting host"	"General adapter problems" "BIOS boot problems"	Windows
"No target devices found or link down message displays in Brocade BIOS Configuration menu"	"General adapter problems" "BIOS boot problems"	Windows
"Unable to boot from the stored boot device settings in the adapter"	"General adapter problems" "BIOS boot problems"	Windows
"Remote LUNs are not visible to the host"	"General adapter problems" "BIOS boot problems"	Windows
"Cannot boot over SAN from installed CNAs or Fabric Adapters"	"General adapter problems" "BIOS boot problems"	Windows
"Boot from SAN may stop on some Hewlett Packard hosts"	"General adapter problems" "BIOS boot problems"	Windows
"Adapter <port id>: BIOS not installed displays during boot process"	"General adapter problems" "BIOS boot problems"	Windows
"VLANs and teams persist after changing port to HBA mode"	"Fabric Adapter problems"	Windows
"HCM not discovering all Ethernet ports for vNICs"	"Fabric Adapter problems"	Windows
"No adapters found on local host" message in HCM"	"HBA problems"	Windows
"Only one adapter port participates in trunk"	"HBA problems"	All
"Quality of Service performance issues"	"HBA problems"	All
"Quality of Service not functioning"	"HBA problems"	All
"Only one adapter port participates in trunk"	"HBA problems" "Trunking problems"	All
"Trunked port disables on the switch"	"HBA problems" "Trunking problems"	All
"Cannot disable trunking"	"HBA problems" "Trunking problems"	All
"Unable to create more than 126 Virtual (NPIV) ports for adapter"	"HBA problems"	All
"Cannot manage CNAs after attempting upgrade to 3.0 drivers"	"CNA problems"	Windows 2003
"VMQs not created for virtual network adapter instances"	"CNA problems"	Windows 2008
"Ethernet loopback test problems"	"Network interface problems (CNA or NIC)"	All

TABLE 2 Isolate adapter problems (continued)

Problem	Category	OS Specific
"Ethernet link ports or LOM not coming up on reboot in Linux"	"Network interface problems (CNA or NIC)"	Linux
"Loss of adapter hardware address in Linux"	"Network interface problems (CNA or NIC)"	Linux
"Loss of adapter IP address in Linux"	"Network interface problems (CNA or NIC)"	Linux
"Network stack runs out of heap"	"Network interface problems (CNA or NIC)"	VMware
"NIC numbering unexpected on VMware systems"	"Network interface problems (CNA or NIC)"	VMware
"Poor network performance"	"Network interface problems (CNA or NIC)"	Linux Windows
"VLAN creation and operation problems"	"Network interface problems (CNA or NIC)"	Windows
"Teaming or VLAN operations through HCM fail"	"Network interface problems (CNA or NIC)"	Windows 2003
"Ping to remote host is failing"	"Network interface problems (CNA or NIC)"	All
"Receive-side scaling disables unexpectedly"	"Network interface problems (CNA or NIC)"	Windows 2008
"Applications using TDI driver stop responding"	"Network interface problems (CNA or NIC)"	Windows 2008 and Windows Vista
"RSS network throughput decreases"	"Network interface problems (CNA or NIC)"	Windows 2008 R2
"SNMP MIB browser not displaying information on VLAN-related OIDs"	"Network interface problems (CNA or NIC)"	Windows
"Teaming errors"	"Network interface problems (CNA or NIC)"	Windows
"BNI driver upgraded, installed, or removed"	"Network interface problems (CNA or NIC)"	Windows
"Binding issues after Hyper-V enabled with teaming"	"Network interface problems (CNA or NIC)"	Windows
"Loss of sync and loss of signal errors in port statistics"	"FCoE and Fibre Channel problems"	All
"Fabric authentication failures"	"FCoE and Fibre Channel problems"	All
"Adapter is not showing in the fabric"	"FCoE and Fibre Channel problems"	All
"Virtual devices not listed in name server"	"FCoE and Fibre Channel problems"	All
"Adapter not registering with the name server or cannot access storage"	"FCoE and Fibre Channel problems"	All

TABLE 2 Isolate adapter problems (continued)

Problem	Category	OS Specific
"FCoE link is down"	"FCoE and Fibre Channel problems"	All
"I/O problem on connected FCoE device"	"FCoE and Fibre Channel problems"	All
"I/Os are not failing over immediately on path failure in MPIO setup"	"FCoE and Fibre Channel problems"	Windows Linux VMware
"Disk I/O requests cause low throughput and high latency on Linux"	"FCoE and Fibre Channel problems"	Linux
"Disk I/O requests cause low throughput and high latency on VMware"	"FCoE and Fibre Channel problems"	VMware
"DCB is not enabled"	"DCB network problems"	All
"Failed to connect to agent on host... error when using HCM"	"HCM and HCM Agent problems"	All
"HCM Agent service cannot start"	"HCM and HCM Agent problems"	Windows Server 2003
"HCM Agent not auto starting if 3.0 driver updated with 2.3 HCM"	"HCM and HCM Agent problems"	Windows
"Unable to completely uninstall HCM"	"HCM and HCM Agent problems"	Windows
"Time on HCM screens does not match system time"	"HCM and HCM Agent problems"	Windows Server 2003

General adapter problems

This section provides possible resolutions for common problems that could occur with installed CNAs, HBAs, or Fabric Adapters. For additional information on troubleshooting problems on mezzanine or expansion card adapters, refer to "Troubleshooting mezzanine card problems" on page 55.

Adapter not reported under server's PCI subsystem

The adapter is installed but not visible as a device in the host system's PCI subsystem.

Verify whether the adapter is visible as a PCI device by executing your host's operating system command to list PCI devices in the system. For details on this command, refer to the "List PCI Devices" row in Table 5 on page 59. If the adapter is not in the device list, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** Adapter slot is disabled in your system's BIOS.

   Action: Examine your system BIOS settings to make sure the slot has not been disabled (Refer to your system's Administration Guide for details on BIOS settings).

2. **Possible Cause:** Card not seated in host system connector properly.

   Action: Reseat the adapter.

3. **Possible Cause:** Host system connector issues.

   Action: Install an adapter of known working condition to determine whether there is a connector malfunction.

   Action: Try installing the adapter into a different slot, if available.

4. **Possible Cause:** Adapter not compatible with host operating system or connected storage systems.

   Action: Verify compatibility by reviewing the *Brocade* interoperability matrices on the Brocade adapters website at www.brocade.com/adapters.

No adapters reported though BCU adapter --list command

If the adapter does not display when the BCU **adapter –list** command is initiated, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** Adapter is not reported under server's PCI subsystem.

   Action: If the adapter is newly detected or the driver has just been installed, you may need to reboot the system for BCU to discover your new adapter.

   Action: Verify if the adapter is visible as a PCI device by executing your host's operating system command to list PCI devices in the system. For details on this command, refer to the "List PCI Devices" row in Table 5 on page 59.

   Action: If the adapter does not appear in the list of PCI devices, refer to "Boot devices not available in host's Boot Manager menu" on page 21 for possible causes and recommended actions.

2. **Possible Cause:** Adapter driver is not loaded.

   Action: Verify if the adapter is visible as a PCI device by executing your host's operating system command to list PCI devices in the system. For details on these commands, refer to the "List PCI Devices" row in Table 5 on page 59.

Port link is not active

The link between the adapter and switch port does not appear to be active because of adapter LED operation (stand-up adapters only), lack of data over the link, or the BCU **port –query** or **port –list** command shows that the link state is down. Refer to "Displaying the port list" on page 103 for more information.

Refer to the following descriptions of possible causes and recommended actions or fixes for the problems:

1. **Possible Cause:** SFP or cable problems (stand-up adapters).

   Action: Ensure that the SFPs and cables are connected properly on both adapter and switch sides. Check for any cable damage.

   Action: Swap the SFP or cable for known working ones.

2. **Possible Cause:** Switch port is disabled or switch is disabled.

   Action: Execute either the Fabric OS **switchShow** or **portShow** commands on the attached switch to ensure that the switch or individual port is not disabled or offline. Use appropriate switch commands to enable the port.

3. **Possible Cause:** Adapter port is disabled.

   Action: Verify port state using the HCM **Port Properties** dialog box or BCU port --list command. Use BCU **port –enable** command to enable the port.

4. **Possible Cause:** Adapter's port speed or topology mismatch with the switch port (HBAs or Fabric Adapter ports configured in HBA mode only).

   Action: Check the port topology setting on the switch using the Fabric OS **portCfgShow** command to ensure that Locked L_Port is OFF. Use the **portCfgLport** command to change the setting to OFF if required.

   Action: Check the switch port speed using the Fabric OS **portCfgShow** command to verify that speed is either AUTO or matches the speed of the attached adapter port (for example, the speed setting for both ports is 4 Gbps).

   Action: Check port speed on the adapter with the BCU **port –list** or **port –query** commands to display the current and configured speed. Refer to "Displaying port speed" on page 103 and "Performing a port query" on page 103 for details on using these commands.

5. **Possible Cause:** Non-Brocade-branded SFP installed (stand-up adapters). If non-Brocade branded SFPs are inserted on the adapter or switch, the port link will not come up.

   Action: On the switch, execute the Fabric OS **switchShow** command to verify that "Mod_Inv" (invalid module) does not display for the port state.

   Action: On the adapter, execute the **port –list** or **port –query** BCU commands to verify display in the **Sfp** field. Refer to "Displaying the port list" on page 103 and "Performing a port query" on page 103. If an unsupported SFP is detected, the **Sfp** field displays "us" (unsupported SFP) for **port –list**, and the **Media** field displays "Unsupported SFP" for **port –query**.

   For additional actions and fixes for the port link not coming up, refer to "Verifying Fibre Channel and DCB links (stand-up adapters)" on page 50.

6. **Possible Cause:** Firmware failure. In most cases this causes a heartbeat failure, and if auto-recovery is enabled, the driver recovers. No corrective action is needed.

   Action: If link does not recover and BCU **port –list** command shows fcoe and eth state is **link down**, download the latest driver package, and then remove and reinstall the package using instructions in the "Software Installation" chapter of the *Brocade Adapters Installation and Reference Manual*. To download the driver package, perform the following steps:

   a. Go to the adapters website at www.brocade.com/adapters.

   b. Navigate to the adapters **Downloads** page.

   c. Select your operating system from the **Downloads** list to display appropriate downloads or download the ISO image.

Device drivers not loading for all adapter instances

On Windows systems, not all adapter instances have device drivers loaded after a driver update. As a result, some of the adapter instances show up in Device Manager with a yellow bang (yellow circle with explanation point). This is more often seen when there are a large number of adapter instances on the server.

Possible Cause: The available memory resources on the server are insufficient to support all adapter instances for the current boot.

Action: Try rebooting the system to force a resource rebalance. If the problem persists, increase the system memory or disable some of the adapter instances.

Installer program does not autorun

On Windows systems, if the installer program does not automatically run from the DVD that you create with the ISO file containing all supported software installation packages, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

NOTE
This ISO file can be downloaded from the Brocade adapters website at www.brocade.com/adapters.

Possible Cause: Autorun is not enabled on your system.

Action: Double-click the "LaunchWinSetup.cmd" file in the root directory of the Installation DVD that you created with the ISO file. This will launch the installer program.

Action: Refer to "Installer program does not autorun" on page 12 for more information to isolate this problem.

Host system freezes or crashes

If the BIOS and the operating system recognize the adapter, but the host system freezes or crashes during startup and does not boot, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Causes:

- Conflicts with adapter port operating speed or topology of attached devices.
- Adapter not compatible with host system.
- Faulty fiber optic cabling and connections (stand-up adapters only).
- Faulty or unseated SFPs or unsupported SFPs (stand-up adapters only).

Action: Disconnect all devices from the adapter, then reboot the host system.

- If the system does not freeze when rebooted and operates correctly, use the following information to resolve the problem:
  a. Check for faulty cable and cable connections.
  b. Try rebooting the system without any connectivity to the switch. This will help isolate any hang caused by switch and device interactions.
  c. Reseat SFPs in the adapter (stand-up adapters only). Determine whether the installed SFPs are faulty by observing LED operation by the adapter ports. If all LEDs are flashing amber, the SFP is invalid and may not be a required Brocade model. You can also verify SFP operation by replacing them with SFPs in a known operating condition. If the problem is resolved after replacement, the original SFP is faulty.
  d. Check for conflicts with attached devices. Verify that data speed and connection topology (for example, point-to-point) for devices attached through the adapter are compatible with settings on the adapter port. Although *auto* may be set, configuring settings manually on the adapter port and devices may allow connection. Also, note that the adapter only supports point-to-point connection topology. Refer to the *Brocade Adapters Administrator's Guide* for procedures to configure adapter ports.

NOTE
Observe the LEDs on adapter ports (stand-up adapters only). Illuminated LEDs indicate connection, link activity, and connection speed negotiated with the attached device. For the meaning of LED operation, refer to the *Brocade Adapters Installation and Reference Manual*.

- If the system freezes perform the following tasks:
  a. Verify whether the host system firmware supports PCIe specifications listed in the *Brocade Adapters Installation and Reference Manual*. If not, download a firmware update to support the adapter.
  b. Verify compatibility by reviewing the Brocade interoperability matrixes on the Brocade adapters website at www.brocade.com/adapters.
  c. On Windows systems, determine when the system freezes during the boot process. If it freezes as the driver loads, uninstall and reinstall the driver. If it freezes during hardware recognition, uninstall both the driver and adapter, then reinstall both.
  d. Remove the adapter and reboot the system. If the system boots, reinstall the adapter.
  e. Reseat the adapter in the host system.
  f. Uninstall and reinstall the driver.
  g. Try installing the adapter into a different compatible slot.
  h. Try installing the adapter into another host system. If the problem does not occur, the adapter may not be compatible with the original host system. If the problem occurs in the new system, replace the adapter.

Action: Refer to "Verifying Fibre Channel and DCB links (stand-up adapters)" on page 50 for more information to isolate this problem on stand-up adapters.

Operating system errors (blue screen)

If critical errors display for the host system and the system blue screen appears, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Adapter driver not loaded.

Action: Refer to "Adapter driver installation verification" on page 51 for methods to verify driver installation.

Driver event messages appearing in host system log files

If event messages for the adapter driver are appearing in the host system log files, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Various causes and severity levels.

Action: Follow the recommended action in the message.

Action: Resolve critical-level messages and multiple major or minor-level messages relating to the same issue as soon as possible.

Action: For details on event messages, refer to "Logs" on page 69.

BCU version mismatch warning

Output from BCU commands has the following warning message.

```
WARNING: BCU and Driver versions don't match !!!
```

Possible Cause: Installation may be incomplete. Either the BCU or one or more driver instances were not upgraded to the latest version.

Action: Remove the driver package, then reinstall. Refer to the "Software Installation" chapter in the *Brocade Adapters Installation and Reference Manual*.

> **NOTE**
> Make sure that the server does not reboot before reinstalling the driver. This will corrupt the installation because, without the driver, the boot LUN cannot be located. To safeguard against a reboot, open an additional remote desktop session to the console or terminal during removal and reinstallation. If a reboot occurs, you will be prompted that others are logged on to the system and asked if you want continue with the reboot.

Action: Refer to "Errors or problems when entering BCU commands".

Possible Cause: In Windows systems, this message may occur if there are redundant entries in the Temporary and Environmental Path string pointing to a previous installation.

Action: For Windows systems, go to **My Computer > Properties > Advanced > Environmental Variables**. Check for a multiple entry for a previous installation in the **Path** variable string. For example, if C:\Program Files (x86)\BROCADE\ADAPTER\driver appears twice in the string, there were two x86 driver installations. You can select **Edit** and remove one of the instances from the string.

Errors or problems when entering BCU commands

Entering a BCU command at your operating system command prompt may yield one of the following results:

- A version mismatch message displays.
- BCU is not recognized as an internal or external command, operable program, or batch file.

Possible Cause: BCU commands are not in directory path because BCU desktop shortcut was created during adapter software installation.

Action: Launch BCU command prompt using Brocade BCU desktop shortcut.

bcu pcifn --list and vhba --query commands return errors

The BCU **pcifn –list** command returns an error titled "ERROR: IOC failure - Retry if persists contact support". Also the **vhba –query** command returns "--" for pcifn bandwidth.

Possible Cause: vhba 0 of port 0 is not enabled.

Action: Make sure that vhba 0 of port 0 is enabled by running the bcu **vhba –enable** command for this vhba and port, and then retry the **pcifn -list** and **vhba -query** commands.

I/O data traffic issues

I/O data traffic issues are occurring, such as an application is not receiving data, FTP problems on an Ethernet network, data is not reaching a target on a Fibre Channel network, or ping failures.

1. **Possible Cause:** Ethernet traffic problem

   NOTE
   This applies to CNAs or Fabric Adapter ports configured in CNA mode.

   Action: Run the Ethernet loopback serdes test on the suspected Ethernet port using the BCU **diag –ethloopback** command. This tests internal adapter hardware components. If the test passes, suspect the following external problems:

   - Faulty fiber
   - Faulty software
   - Destination host problem

   Action: Run the BCU Ethernet external loopback test using the BCU command **diag –ethloopback** command (stand-up adapters only). Be sure that a loopback connector is installed in the port. If the serdes or internal loopback test passes, but the external test fails, suspect the following problems:

   - Loopback connector not inserted in transceiver
   - Faulty SFP or loopback connector.

2. **Possible Cause:** Fibre Channel or FCoE I/O problems.

   NOTE
   This applies to CNAs, HBAs, and Fabric Adapter ports configured in CNA or HBA mode.

   Action: Run the loopback serdes test on the suspected Fibre Channel port (HBA port) or FCoE port (CNA port) using the BCU **diag –loopback <port_id> -t serdes** command. If the test passes, suspect the following external problems:

   - Faulty fiber
   - Faulty software
   - Target problem

   Action: Run the BCU external loopback test (stand-up adapters only) using the BCU command **diag –loopback <port_id> <pattern>**. Be sure that a loopback connector is installed in the port. If the serdes or internal loopback test passes, but the external test fails, suspect the following problems:

   - Loopback connector not inserted in transceiver
   - Faulty SFP or loopback connector.

Support Save file is too large (Windows only)

The Support Save file is getting too large (it may be larger than 1 Gb).

Possible Cause: The hbaagent.log file may be exceeding its maximum size.

Action: Delete the larger files, especially hbaAgent.log if it exceeds 10 Mb, in the following location, and then run Support Save again

C:\Program Files\BROCADE\Adapter\driver\util\hbaagent\log\

Host system running Microsoft Windows fails to hibernate

A host system with Microsoft Windows and a Brocade adapter fails to go into hibernation mode with the following message:

The following items are preventing hibernation on this system.

The system does not support hibernation.

The storage drivers do not support hibernation."

Possible cause: Microsoft hotfix KB932755 has not been installed on the server. This happens if the adapter driver was installed through a driver update disk (DUD). The DUD does not perform the prerequisite checks as part of installation.

Action: Install the KB932755 hotfix.

Driver incompatible with CNA drivers

Installing 3.0 release Windows 2003 installation fails with “This driver package is incompatible with Brocade CNA drivers” message.

Possible Cause: Windows 2003 is not supported for CNAs in Release 3.0.

Actions

- If the system has only CNAs

  Install release 2.3.x.x drivers for CNAs (1020, 1010, 1007, 1741). Windows 2003 drivers for CNAs are included in subsequent releases.

- If the system has both HBAs and CNAs

  Uninstall the CNA drivers then install 3.0 drivers to manage the HBAs.

If both adapters need to be managed simultaneously, you must use the pre-3.0 release drivers

Brocade BCU desktop shortcut missing (Windows only)

BCU desktop shortcut not visible on system desktop.

Possible Cause: Shortcut was deleted or not installed with adapter software.

Action: Re-install the adapter driver package with the software installer command for your system and, using the DFORCE option. Reboot the host system if required.

Action: Create the shortcut again manually. To create the shortcut on Windows systems, use the following steps.

1. Go to the C:\Program Files\Brocade\Adapter\driver\util directory.

   NOTE
   This is the location of the BCU executable (bcu.exe) if it is installed and the default location was selected during installation.

2. Right-click bcu.exe and select **Send to Desktop**. to create a shortcut.

Driver installation fails and system cannot be booted

Installation of a new Windows 2008 driver package fails in systems where an adapter is used for booting over SAN and the operating system becomes unbootable.

Possible Cause: Existing driver package that was accessing the remote boot LUN was removed and system was rebooted.

Action: Install the new adapter driver without uninstalling the existing driver. This is the recommended procedure for updating adapter drivers.

NOTE
If you remove the adapter driver (which requires a system reboot because the adapter was modified), and then reinstall the driver, installation will fail because the operating system cannot update the driver while a system reboot is pending. However, if you reboot the system after removing the driver, the operating system will not come up because the driver accessing the operating system was removed.

Cannot remove Linux driver with uninstaller application or scripts

When removing the Linux driver package using the Brocade Software Uninstaller application or script command (**brocade_install_rhel.sh -u**), the network (bna) or storage (bfa) driver will not uninstall, and a message such as the following will display:

```
Uninstalling the Brocade driver <version> RPM's
Unloading bna driver ...
ERROR: Module BNA could not be unloaded; Uninstall terminated!
```

Possible Cause: An application such as HCM may be running and accessing the bna or bfa driver module. Execute the **rmmod bna** or **rmmod bfa** command and verify that the following displays:

```
ERROR: Module bna is in use
```

or

```
ERROR: Module bfa is in use
```

Action: Run the **fuser -v /dev/bfa** and **fuser -v user/dev/bna** commands to list the PIDs and names of processes accessing the bfa or bna modules. Kill the processes accessing these modules and then retry driver removal.

Removing Ethernet (network) drivers causes error

NOTE
This applies to CNAs or Fabric Adapter ports configured in CNA or NIC mode.

When removing Ethernet or network drivers on Windows systems and no previous drivers are installed, the following occurs:

- The install log displays the following intermediate error message.

  ```
  Error = 6, Failed to unistalled device instance ID.....
  ```

- The adapters disappear from the Device Manager as network devices.

Possible Cause: Normal behavior for Windows systems.

Action: Take the following actions:

- Rescan for the devices in the Device Manager.
- Ignore the error message.

Files needed for bfad.sys message appears

If a “Files needed for bfad.sys” message appears on Windows systems when removing a driver, refer to the following possible cause and recommended action to help resolve the problem.

Possible Cause: A “Files needed for bfad.sys” message will occur if you perform the following sequence of steps.

1. Install the driver using the driver installer program (brocade_installer.bat) or Brocade Adapters Software Installer (GUI or command-based application).
2. Uninstall the Brocade adapter using Windows Device Manager.
3. Re-install the driver using the driver installer program (brocade_installer.bat) or Brocade Adapters Software Installer (GUI or command-based application).
4. Uninstall the driver using the driver installer program (brocade_installer.bat) program.

Action: To avoid the message when removing a driver, do not uninstall the driver using the Device Manager if you have used Brocade installer driver installer programs to install driver instances. Always use the Brocade installer programs. If only one driver is present in the system, then the Brocade programs also remove the Fibre Channel devices from the Device Manager.

Cannot roll back driver on all adapter instances using Device Manager

If you cannot roll back the driver for all adapter instances using Windows Device Manager, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Installing the driver using the Brocade driver installer program (brocade_installer.bat) or Brocade Adapters Software Installer (GUI or command-based application), then rolling back driver adapter instances using the Device Manager.

Actions: Perform the following actions:

- Install the driver for each adapter instances using the Device Manager, then roll back the driver using Device Manager.
- Use the driver installer script (brocade_installer.bat) or Brocade Adapter Software Installer (GUI or command-based application) to install or upgrade the driver, then use the Brocade Software Uninstaller to roll back drivers on all adapter instances in one step.

Device drivers not loading due to lack of MSI-X interrupt vectors

Due to a lack of MSI-X interrupt vectors on VMware systems, device drivers are not loading completely as not enough vectors are available for proper operation.

Possible Cause: A large number of adapters and other devices in the system causes the operating system to run out of MSI-X interrupt vectors. This is most visible in ESX 4.x where VMware supports up to 224 interrupt vectors shared by all the devices.

1. **Action:** Reassess the hardware configuration and distribute the adapters so no more than four 10Gbps Ethernet ports are used in a single system (maximum supported by VMware). This VMware limitation applies to Brocade CNA ports and Fabric Adapter ports configured in CNA mode.
2. **Action:** If there are a large number of Brocade HBA ports or Fabric Adapter ports configured in HBA mode in the system, try disabling MSI-X mode for Brocade ports using the following commands.
   a. Enter the following command to display current driver configuration settings, including default options.

      ```
      esxcfg-module -g bfa
      ```

   b. Append "msix_disable_cb=1" to the default options displayed by the preceding command:

      ```
      esxcfg-module -s "<default_options> msix_disable_cb=1" bfa
      ```

NOTE
Disabling MSI-X mode can reduce performance so any performance critical tasks should be done with a smaller number of adapters in the system, in order to utilize the MSI-X mode.

Driver installation fails on ESX systems

Driver(s) are not installing on VMware ESX system. If installing through HCM, the following error message may display when updating drivers.

```
Uploading of the driver file is failed. Reason - Maintenance mode is not enabled
or could not be determined.
```

Possible Cause: ESX systems must be in maintenance mode to install or update drivers.

Action: Place system in maintenance mode, then reinstall driver plackage(s).

Errors when using GUI-based software installer

Errors occur when launching the GUI-based Brocade Adapter Software Installer, such as InvocationTargetException errors

Possible Cause: Your system may not be able to run a GUI-based application.

Action: Use the Software Installer commands detailed in the *Brocade Adapters Installation and Reference Manual*.

Errors when installing brocade_driver_linux_<versions>.tar.gz package

If errors occur when installing the no architecture (noarch) brocade_driver_linux_<versions>.tar.gz driver package, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Appropriate distribution kernel development packages are not installed on your host system for the currently running kernel.

Action: If you are installing the brocade_driver_linux_<versions>.tar.gz driver package, the driver module compiles on the system during installation. If driver build errors result when you install the package, verify that the appropriate distribution kernel development packages are installed on your host system for the currently running kernel. These packages should include the gcc compiler and the kernel sources. If these are not installed, you will need to install them through your Linux OS Software Management tools or reinstall the operating system before you can continue the driver installation. Be sure to "install everything" including the developer library options.

UEFI boot problems

This section describes problems that may occur when using the Brocade adapter and unified extensible firmware interface (UEFI) for booting a host system from a remote storage device (boot over SAN). Possible causes and recommended actions to help resolve the problems are provided.

System will not boot over SAN or on local disk in Legacy BIOS mode

On some IBM UEFI based systems, **Hard Disk 0** is not present after **Legacy Only** option in boot manager and system will not boot as local disk or over SAN.

Possible Cause: Hard Disk are not present in the boot manager list.

Action: Follow these steps:

1. Press F1 to enter **System Setup** during early phase of booting.
2. Select **Boot Manager** and press Enter.
3. Select **Add Boot Option** and press Enter.
4. Select **Legacy Only** and press Enter.
5. Press Esc to return to Boot Manager.
6. Select **Change Boot Order** and press Enter.
7. Select the existing **Boot Order** and press Enter.
8. Select **Legacy Only** and press the + key to promote the boot order to a position above the local device that contains the operating system (typically, this would be above Hard Disk 0). Press Enter.
9. Confirm that Hard Disk 'x' is present in the list. If not, return to step 3 and add **Hard Disks** to the boot order.
10. Select **Commit Changes** and press Enter.
11. Press Esc to return to Boot Manager.
12. Select **Reset System** and press Enter.

Host not booting from remote LUN

If the host system where the adapter is installed does not boot from the remote boot LUN, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Boot over SAN is not configured correctly.

Action: If booting the host from a remote boot device, verify whether “boot over SAN” configuration is complete and correct. For example, verify the following:

- A zone is created on the attached switch that contains only the PWWN of the storage system port for the boot LUN and the PWWN of the adapter port.
- BIOS or EFI is enabled to support boot over SAN from a specific adapter port.
- BIOS or EFI is configured to boot from a specific LUN.
- The host’s operating system, adapter driver, and other necessary files are installed on the boot LUN.

Boot devices not available in host’s Boot Manager menu

Fibre Channel attached boot devices do not appear in the EFI Boot Manager menu or a boot device appears, but it is not functioning. Following are descriptions of possible causes and recommended actions or fixes for the problem.

1. **Possible Cause:** The adapter is not seated properly in the host system.

   Action: Select the EFI Shell from the EFI Boot Menu and use the **devices** command to determine if EFI has detected the Brocade adapter.

   A Brocade adapter will have “Brocade Fibre Channel” in the device name. A CNA or Fabric Adapter port configured in CNA mode will also have “Brocade Ethernet Controller” in a device name.

   If the adapter is not listed, perform the following steps:

   - Reseat the adapter.
   - Replace the adapter with an adapter in known working condition to determine whether there is a host connector malfunction.

2. **Possible Cause:** Adapter connector problems in host.

   Action: Perform the following steps.

   a. Reseat the adapter.

   b. Replace the adapter with an adapter in known working condition to determine whether there is a host connector malfunction.

   c. Reinstall the adapter in a different host connector.

3. **Possible Cause:** The adapter is not compatible with the host operating system or connected storage systems.

   Action: Verify compatibility by reviewing the interoperability matrixes on the Brocade adapters website at www.brocade.com/adapters.

4. **Possible Cause:** No Fibre Channel attached drives are available from the attached Fibre Channel switch.

   Action: Check for attached disk devices.

   a. Use the **devices** EFI shell command to display the detected devices.

      A Brocade adapter may display as the following.

      ```
      29 B X -  1  2  8 Brocade Fibre Channel HBA
      ```

"29" is the device handle, and will be different in most systems. More than one Brocade adapter may display.

b. Use the EFI shell **dh** command to display additional information about each Brocade adapter. This will include any attached Fibre Channel disk devices. For example, you would enter the following for the HBA or Fabric Adapter port configured in HBA mode with device handle 29:

```
Shell> dh -d 29
```

The following displays:

```
29: PciIo ScsiPassThruExt BusSpecificDriverOverride DevPath
(..P0A08,300)/Pci(0|0)/Pci(0|0))
...
     Managed by :
       Drv[25] : Brocade Fibre Channel Adapter Bus Driver
       Drv[26] : SCSI Bus Driver
...
     Child Controllers  :
       Child[70] : SCSI Disk Device
       Child[71] : SCSI Disk Device
       Child[72] : SCSI Disk Device
```

The SCSI Disk Devices under "Child Controllers" are the LUNs that the Fibre Channel adapter can access.

c. If an expected Fibre Channel attached disk does not appear in the "dh -d" list for a Brocade adapter, check the cabling, the adapter's link status LEDs, and the Fibre Channel switch configuration.

NOTE
The Brocade adapter port may have been disabled with the EFI shell **drvcfg** command. Use the **drvcfg -s** shell command to check the enabled status and configuration of the port, including the requested speed. After entering **drafted -s**, select the appropriate adapter from the **Adapter List** screen and press **Enter** to view and modify port properties.

Driver and operating system installation failure on boot LUN

Installation fails when installing drivers with the driver update disk (DUD) and an installing operating system to a remote LUN being used for booting over SAN.

Possible Cause: The appropriate driver update disk (DUD) may not have been used for the host operating system and platform. For example, if the brocade_adapter_rhel53_x86_64 DUD is used during RHEL 5.3 x86 installation, installation will fail.

Action: Download the appropriate DUD for your host platform from the Brocade adapters website using the following steps.

1. Go to the adapters website at www.brocade.com/adapters.
2. Navigate to the adapters **Downloads** page.
3. Select your operating system from the **Downloads** list to display appropriate downloads.
4. Download the dud from the "Driver Update Disk (DUDs)" area.

Driver preinstallation problems

The following problems may occur when drivers are preinstalled to your Windows host system driver store.

Preinstallation failed when attempted twice in a row without inserting adapters

Preinstallation of drivers fail when attempted twice in a row and adapters are not inserted in the system.

Possible Cause: Windows restricts upgrading a preinstalled driver before installing the hardware.

Action: Remove the driver package that was preinstalled earlier, then retry preinstalling the new driver package.

Preinstallation with adapter installed in system does not update the installed driver image

Preinstallation does not update the currently installed driver image when an adapter is already present in the system.

Possible Cause: This is an expected behavior in Windows. You must install (instead of preinstall) the driver to update the currently loaded driver if the hardware is already present on the system.

Action: Reinstall the driver using **brocade_install.bat** installer script command with the FORCED_INSTALL=TRUE option.

Installing Windows 2008 R2 DUD on UEFI system results in offline disk

Installing the Windows 2008 DUD and operating system on a formatted UEFI system disk that you are configuring as a bootable device results in an offline disk.

Possible Cause: This behavior is working as designed by Microsoft if the disk is formatted, as the default SAN POLICY is OFFLINESHARED, which marks SAN disks as Read Only during setup to ensure that no data center related data are accidentally overwritten.

Action: Use an unformatted “fresh” disk for DUD and operating system installation. Also refer to the “How to Use Windows Setup to Install Windows with UEFI Support” section of the *Microsoft UEFI Guide*.

BIOS boot problems

This section describes problems that may occur when using the Brocade adapter and Basic Input/Output System (BIOS) for booting a host system from a remote storage device (boot over SAN). Possible causes and recommended actions that may fix the problems are provided.

Driver and operating system installation failure on boot LUN

When installing drivers using the driver update disk (DUD) and an operating system to a remote LUN being used for booting over SAN, the installation fails.

Possible Cause: The appropriate DUD may not have been used for the host operating system and platform. For example, if the brocade_adapter_rhel53_x86_64 DUD is used during RHEL 5.3 x86 installation, installation will fail.

Action: Verify the DUD for your system using information in Chapter 1 of the *Brocade Adapters Installation and Reference Manua*l. Using the correct DUD, reinstall appropriate drivers and the operating system as necessary.

Target not visible from host

If the storage target configured for containing the boot LUN is not visible from the host, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** No fabric connectivity between adapter and target or target is not online.

   Action: Execute the Fabric OS **nsAllShow** command on the attached switch to verify that the target and the host are online in the fabric and registered in the name server.

2. **Possible Cause:** The target and the adapter are not on the same zone.

   Action: Execute the Fabric OS **cfgActvShow** command on the attached switch and verify that the host and target are in the same zone (either using domain area members, port area members, or port or node WWNs).

3. **Possible Cause:** The adapter driver is not loaded.

   Action: The adapter driver may not be loaded. Refer to "Adapter driver installation verification" on page 51 for methods to verify driver installation

4. **Possible Cause:** There is a problem with the remote port.

   Action: Verify that the remote target port (rport) is reporting itself online by comparing rport online and rport offline statistics. Refer to "Remote port statistics" on page 84 for details on displaying these statistics. The rport online counter should be one greater than the rport offline counter. If not, clear the counters and try connecting to the remote port again. Verify the rport online and rport offline statistics again.

Ctlr-B option does not display when booting host

When booting the host, the Ctrl-B option does not display so that you can access the **BIOS Configuration** menu.

Possible Cause: The adapter might not be loaded with the latest adapter boot image (bfa_boot_fw). Download the latest boot code image for installed Brocade adapters from the Brocade adapters website using the following steps.

1. Go to the adapters website at www.brocade.com/adapters.
2. Navigate to the adapters **Downloads** page.
3. Select your operating system from the **Downloads** list to display appropriate downloads.
4. Download the boot code image from the "Boot Code" area.

NOTE
For instructions on updating the boot image, refer to the "Boot Code" chapter in the *Brocade Adapters Installation and Reference Manual*.

Possible Cause: Due to memory constraints system BIOS might not be able to execute the Brocade adapter option ROM.

Action: Disable option ROM on several add-in cards installed in system.

No target devices found or link down message displays in Brocade BIOS Configuration menu

"No target devices found or link down" message displays on Brocade BIOS configuration menu during boot device discovery.

1. **Possible Cause:** There is no fabric connectivity between the Brocade adapter and target, or the target is not online.

   Action: Execute the Fabric OS **nsAllShow** command on the attached switch to verify that the target and the host are online in the fabric and registered in the name server.

2. **Possible Cause:** The target and the adapter port are not on the same zone.

   Action: Execute the Fabric OS **cfgActvShow** command on the attached switch and verify that the host and target are in the same zone by using either domain area members, port area members, or port or node WWNs.

3. **Possible Cause:** The link between the adapter port and target is not active yet.

   Action: Check that the speeds for the adapter port and the connected switch port match. The best approach is to set both speeds to "auto" or "autonegotiate."

Unable to boot from the stored boot device settings in the adapter

The host is unable to boot from the boot device settings stored in the adapter. A "No boot LUNs configured" message will display next to the adapter value when booting.

1. **Possible Cause:** In the Brocade BIOS Configuration Utility, the **Boot LUN** field In the **Adapter Settings** screen is set to **Auto Discover** or **First LUN**.

   Action: Change the **Boot LUN** setting on the **Adapters Settings** screen to **Flash Values.** Refer to the Boot Code chapter in the *Brocade Adapters Installation and Reference Manual* for details.

2. **Possible Cause:** In HCM, the boot option is set to **Auto Discovered from Fabric** or **First Visible LUN** in the **Boot over SAN** dialog box.

   Action: Change the boot options to **User Configured LUNs** in the **Boot Over SAN** dialog box. Refer to the "Boot Code" chapter in the *Brocade Adapters Installation and Reference Manual* for details.

Remote LUNs are not visible to the host

If LUNs from which the host system will boot are not visible from the host system, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** The driver update disk (DUD) used to install the driver and necessary file structure on remote LUNs for boot over SAN operation is not correct for the host operating system being installed on the LUN.

   Action: Download and install the correct the driver update disk for the OS that is being installed from the Brocade adapters website using the following steps:

   a. Go to the adapters website at www.brocade.com/adapters.

   b. Navigate to the adapters **Downloads** page.

   c. Select your operating system from the **Downloads** list to display appropriate downloads.

d. Download the dud from the “Driver Update Disks (DUDs)” area.

2. **Possible Cause:** Missing or improper storage array LUN mask setting.

   Action: Check LUN mapping and masking using the storage array configuration applications.

3. **Possible Cause:** Missing or improper storage array LUN mask setting.

   Action: Check LUN mapping and masking using storage array configuration tools.

4. **Possible Cause:** Adapter driver not loaded.

   Action: The adapter driver may not be loaded. Refer to “Adapter driver installation verification” on page 51 for methods to verify driver installation.

Cannot boot over SAN from installed CNAs or Fabric Adapters

You cannot boot over SAN from CNAs or Fabric Adapter ports configured in CNA mode. However, you can boot from HBAs or Fabric Adapter ports configured in HBA mode installed on the same system.

Possible Cause: A maximum of four boot LUNs are exported to the system. Boot LUNs connected through HBAs and Fabric Adapter ports configured in HBA mode take precedence over boot LUNs connected through CNAs or Fabric Adapter ports configured in CNA mode. If all four boot LUNs are connected through HBAs or Fabric Adapter HBA ports, boot over SAN will not occur through installed CNAs or Fabric Adapter CNA ports.

Action: If you want to boot over SAN through a CNA or Fabric Adapter port configured in CNA mode, disable BIOS on all installed HBAs. To disable BIOS, use BCU commands, the BIOS configuration utility, or HCM. Refer to the “Boot Code” chapter in the *Brocade Adapters Installation and Reference Manual* for instructions.

Boot from SAN may stop on some Hewlett Packard hosts

The boot process may stop on some Hewlett Packard systems, such as the HP DL180, and the following message displays.

```
02a2: BMC System Error Log (SEL) Full`
/Press F1 to Continue, Press F2 to Setup/
```

Possible Cause: The System Event Log may become full of erroneous IPMI (intelligent platform management interface) events reported by the system BIOS.

Action: Perform the following steps.

1. Boot the server and press **F10** when prompted to run BIOS Setup.
2. Select the **Advanced** menu.
3. Scroll down to **IPMI** and press **Enter**.
4. Scroll down to the **System Event Log** selection and press **Enter**.
5. At the **Clear System Event Log** selection, press **Enter** to toggle between **Enable** and **Disable**.
6. Select **Enable**.
7. Press **F10** to save the changes and exit the BIOS Setup.

NOTE
Action: Refer to *Hewlett Packard (HP) Customer Advisory Document* c01199684 on the HP technical support website for detailed information.

Adapter <port id>: BIOS not installed displays during boot process

An “Adapter <port id>: BIOS not installed” message displays when booting from an adapter.

Possible Cause: Either the boot image is not present in the adapter option ROM or initialization of the adapter failed for some reason.

1. Boot image is not present in the adapters.
2. Adapter might have failed to initialize.
3. Link did not come up.

Action: Bring up the host system either using the Brocade live DVD or boot from local disk.

Action: Download the latest boot code image for installed Brocade adapters from the Brocade adapters website using the following steps.

1. Go to the adapters website at www.brocade.com/adapters.
2. Navigate to the adapters **Downloads** page.
3. Select your operating system from the **Downloads** list to display appropriate downloads.
4. Download the boot code image from the “Boot Code” area.

NOTE
For instructions on updating the boot image, refer to the “Boot Code” chapter in the *Brocade Adapters Installation and Reference Manual*.

Fabric Adapter problems

This section provides information for resolving problems more specific to Fabric Adapters. For additional information on troubleshooting problems on mezzanine card adapters, refer to “Troubleshooting mezzanine card problems” on page 55.

VLANs and teams persist after changing port to HBA mode

If a vNIC is configured on a port that is in CNA or NIC mode and a VLAN or team is configured with the vNIC, the VLAN or team will persist if the user changes the port to HBA mode. The VLAN or team will continue to display in the Device Manager and will persist even after reboot. This is because the network driver will not reload after changing the port to HBA mode.

Possible Cause: Port is changed from CNA or NIC mode to HBA mode and network driver is not reloaded on system reboot.

Action: Ensure that all the teams and VLANs are removed from the port before changing from CNA or NIC mode to HBA mode.

HCM not discovering all Ethernet ports for vNICs

vNICs are created for adapter on Windows systems, but HCM is not discovering all related Ethernet ports.

Possible Cause: Agent started before network driver came online to discover ports.

Action: Restart **Brocade HCM Agent Service** from Windows **Services** window.

HBA problems

This section provides information for resolving problems more specific to functions of HBAs or Fabric Adapter ports configured in HBA mode. For additional information on troubleshooting problems on mezzanine card and expansion card adapters, refer to "Troubleshooting mezzanine card problems" on page 55.

No adapters found on local host" message in HCM

When trying to access adapters on local Windows host through HCM, a "no adapters found on local host" displays.

1. **Possible Cause:** HBA itself is not present, but the driver is installed.

   Action: Verify if the adapter is visible as a PCI device by executing your host's operating system command to list PCI devices in the system. For details on this command, refer to the "List PCI Devices" row in Table 5 on page 59.

   Action: If the adapter does not appear in the list of PCI devices, refer to "Boot devices not available in host's Boot Manager menu" on page 21 for possible causes and recommended actions.

2. **Possible Cause:** Driver was removed from the device manager.

   Action: Confirm driver installation using instructions under "Confirming driver package installation in Windows systems" on page 52. If driver is not installed, use instructions in the *Brocade Adapters Installation and Reference Manual* to install it.

Quality of Service performance issues

If enabling Quality of Service (QoS) is causing poor performance or QoS does not appear to be functioning, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

NOTE
QoS is not supported on CNAs or Fabric Adapter ports configured in CNA mode.

1. **Possible Cause:** One or both of the required licenses are not installed on the edge switch connected to the HBA port or Fabric Adapter port configured in HBA mode:
   - Adaptive Networking (AN) license.
   - Server Application Optimization (SAO) license.

Action: Enter the **bcu qos –query** command for the adapter port connected to the switch. If the QoS state is “Unknown” instead of “Online” and total BB-Credits is “zero,” licenses may not be installed. Verify if licenses are installed by executing the Fabric OS **licenseshow** command on the switch. Install licenses as required.

For more information about Fabric OS commands and QoS support, refer to the *Fabric OS Administrator’s Guide*.

2. **Possible Cause:** QoS is not enabled on both switch and adapter port.

   Action: Verify if QoS is enabled for an adapter port using the **qos -query <port_id>** BCU command. Verify if it is enabled on the switch using the **islShow** command.

   Action: Verify zones on the switch using the Fabric OS **cfgActvShow** command.

3. **Possible Cause:** QoS zones are not created properly on the switch for high, medium, and low priority targets.

   Action: Verify that QoS is configured on the switch using instructions in the *Fabric OS Administrator’s Guide*.

Quality of Service not functioning

NOTE
QoS is not supported on CNAs or Fabric Adapter ports configured in CNA mode.

Quality of Service (QoS) is enabled on an adapter port connected to a supported edge switch, but it does not appear to be functioning.

Possible Cause: The following licenses must be installed:

- Adaptive Networking (AN) license.
- Server Application Optimization (SAO) license.

Action: To determine if these licenses are installed on the connected switch, execute the Fabric OS **licenseshow** command on the switch. If licenses are not installed, install them. For more information about Fabric OS commands and QoS support, refer to the *Fabric OS Administrator’s Guide*.

Trunking problems

This section provides information to resolve problems when N_Port trunking is enabled on adapters.

Only one adapter port participates in trunk

Only one port on the adapter configured for trunking is participating in the trunk.

1. **Possible Cause:** The adapter ports are connected to switch ports in different trunk groups. ports participating in trunking should be connected to the same port group on the switch.

   Action: Connect both adapter ports to the same port group on the switch.

2. **Possible Cause:** Only one adapter port is connected to the switch. The other port is down or not connected.

   Action: Make sure other port is enabled and connected to switch.

3. **Possible cause:** Required licenses not installed on the connected switch.

   Action: Verify if licenses are installed by executing the Fabric OS **licenseshow** command on the switch. Install licenses as required

   Action: Install the following licenses on the switch if necessary.

   - Server Application Optimization (SAO) license
   - Trunking license

NOTE
The switch where the HBA or Fabric Adapter port configured in HBA mode connects must be running Fabric OS 4.6.1 or greater.

Trunked port disables on the switch

One of the trunked ports gets persistently disabled on the switch.

Possible cause: Trunking is not enabled and configured on the adapter.

Action: Enable trunking on the adapter. Follow procedures in the *Brocade Adapters Administrator's Guide*.

Cannot disable trunking

Cannot disable trunking.

Possible cause: Trunking is not disabled on switch and the adapter.

Action: Disable trunking following procedures in the *Brocade Adapters Administrator's Guide.*

Unable to create more than 126 Virtual (NPIV) ports for adapter

If you cannot configure more than 126 N-Port ID Virtualization (NPIV) ports (maximum is 255 for Fibre Channel) refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: The maximum NPIV limit for the connected switch has been reached.

Action: Execute the Fabric OS **configure** command on the attached switch and change the maximum logins per port parameter under the **F_Port login parameters** menu to increase the maximum NPIV IDs allowed per port.

CNA problems

This section provides information for resolving problems more specific to functions of CNAs or Fabric Adapter ports configured in CNA mode. For additional information on troubleshooting problems on mezzanine card and expansion card adapters, refer to "Troubleshooting mezzanine card problems" on page 55.

Cannot manage CNAs after attempting upgrade to 3.0 drivers

On Windows 2003 systems with both HBAs and CNAs installed, BCU and the HCM Agent cannot manage the CNA adapter. This occurs after attempting to upgrade to 3.0 drivers. Since network drivers are not supported on Windows 2003 platforms for version 3.0, only storage drivers install. The upgrade fails with an error message.

If you have specified the same installation location as the previous driver, entering BCU commands will result in the following message. In addition, CNA adapters may disappear from HCM application.

WARNING: BCU and Driver versions don't match!!!

Possible Cause: The 3.0 driver package was extracted to the same folder used for the previous driver version. If this occurs, all the binaries prior to version 3.0 will be replaced by the 3.0 binaries.

Action: To avoid this problem before upgrade, extract the 3.0 driver package to a different location than used for the previous driver package. If you have upgraded and the problem exists, extract the older driver package (prior to version 3.0). This restores the binaries and BCU and HCM should work as expected.

VMQs not created for virtual network adapter instances

Virtual Machine Queue (VMQ) support is enabled on the adapter and Virtual Network optimization is enabled in properties for the virtual machine (VM). When VM is started, the **BCU vnic -query display** command does not confirm VMQ creation.

Possible causes:

1. The shared memory resources reserved for VQM creation is insufficient to support the number of Virtual Machines.
2. VMQ is disabled on the management operating system.

Actions:

1. Try changing the jumbo packet size to a smaller value or configure less receive buffers.
2. Create a sub-key "TenGigVmqEnabled" under the registry hive HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\VMSMP\Parameters on the management operation system.

NOTE
Note that VMQ support is only available on systems running windows Server 2008 R2.

Network interface problems (CNA or NIC)

Use the following information to isolate problems that are more specific to the function of a CNA or Fabric Adapter port configured in CNA or NIC mode. For additional information on troubleshooting problems on mezzanine and expansion card adapters, refer to "Troubleshooting mezzanine card problems" on page 55.

NOTE
Switch command examples used in this section are for the Brocade 8000 Switch.

Ethernet loopback test problems

Errors occur during BCU Ethernet loopback tests.

1. **Symptom:** Loopback test returns "Check link/cable or SFP" error when executed with *-t cable* option (stand-up adapters only).

   Possible Cause: Loopback cable not inserted in tested port.

   Action: Verify that loopback cable is securely inserted in the port that you are testing.

2. **Symptom:** Loopback test returns a "port not disabled" error.

   Possible Cause: Port is enabled.

   Action: Disable the port using the **port –disable** BCU command before running loopback test.

3. **Symptom:** Loopback test returns a "port not disabled" error. The error.displays even after disabling the port.

   Possible Cause: Network load balancing service is enabled. This will cause the adapter to disable and enable, and the previously configured state (port disable) is lost.

   Action: Disable network load balancing and retest.

4. **Symptom:** The loopback test returns "Device busy - Retry operation" or "diag busy."

   Possible Cause: Other users or sessions are running another instance of loopback tests.

   Action: Check if instances of this diagnostic are running using **ps -ef** for Linux and VMware, and Task Manager for Windows systems.

   Action: If instances are still running, wait a few minutes, then again check if the tests done using the **ps -ef** command or Task Manager.

5. **Symptom:** The loopback test returns "Missing frame check and replace SFP/cable" (stand up cards only).

   Possible Cause: The loopback cable was pulled during the test and the test is run in external mode (not serdes mode).

   Action: Restart the test with the cable connected.

Ethernet link ports or LOM not coming up on reboot in Linux

The host system's LAN on motherboard (LOM) is not coming up or ports are not visible after rebooting Linux host.

1. **Possible Cause:** A ifcfg-ethX script is not configured to bring up each LOM and CNA during the system boot process.

   Action: Make sure that a script is configured for each adapter and LOM once drivers are installed. Scripts are located in the following directories:

   - SLES - /etc/sysconfig/network
   - RHEL - /etc/sysconfig/network-scripts

2. **Possible Cause:** NetworkManager is enabled. There are known issues with NetworkManager managing multiple NICs in some Linux distributions.

   Action: Disable NetworkManager.

   To check if NetworkManager is running, enter either of the following commands:

   - chkconfig --list | grep NetworkManager
   - nm-tool

   To disable NetworkManager for RHEL 5 systems, enter the following commands.

   ```
   chkconfig NetworkManager off
   chkconfig NetworkManagerDispatcher off
   ```

   To disable NetworkManager for SLES systems, perform the following steps.

   a. Open YaST.

   b. Select the **Network Devices Network Card**.

   c. On the first screen set the **Network Setup Method** option to **Traditional Method with ifup**.

Loss of adapter hardware address in Linux

The **ifconfig** command displays, HW Addr as 00:00:00:00:00:00.

Possible Cause: The adapter failed to initialize.

Action: Disable the Ethernet I/O controller by entering the BCU **vnic –disable** command, then enable the I/O controller by entering the BCU **vnic –enable** command.

Loss of adapter IP address in Linux

The IP address set in Linux with the **ifconfig** command disappears when the adapter goes down or host system reboots.

1. **Possible Cause:** The IP address was set with the **ifconfig** command and the adapter is enabled in DHCP (Dynamic Hardware Configuration Protocol) mode.

   Action: Configure IP address using system GUI-based networking tools.

2. **Possible Cause:** The IP address is not configured in the ifcfg-ethX script.

   Action: Manually configure IP address in ifcfg-ethX script.

Network stack runs out of heap

The network stack on VMware systems is running out of heap space.

Possible Cause: Enabling NetQueue and using jumbo frames has caused the network stack to run out of heap with default values set for netPktHeapMaxSize and netPktHeapMinSize. Leaving default values can result in unpredictable behavior.

Action: Perform the following steps.

1. Log in to the VI Client.
2. Click the **Configuration** tab for the ESX Server host.
3. Click **Advanced Settings**.
4. Click **VMkernel**.
5. Find the corresponding value field for VMkernel.Boot.netPktHeapMaxSize, and enter 128.
6. Find the corresponding value field for VMkernel.Boot.netPktHeapMinSize, and enter 32.
7. Click **OK** to save the changes.
8. Reboot the system.

NIC numbering unexpected on VMware systems

After installing adapter drivers on VMware systems, NIC numbering is not what is normally expected. For example, instead of vmnic32 or vmnic33, the number is vmnic2 and vmnic3.

Possible Cause: Adapter hardware was installed before drivers.

Action: When installing a CNAs or Fabric Adapters with ports configured in CNA or NIC mode on a VMware systems, it is advisable to install the driver before the adapters so that the NICs will be properly enumerated in the system. To resolve the problem, you must perform the following steps.

1. Uninstall the drivers.
2. Remove the adapter.
3. Reboot your system without the adapter.
4. Install the drivers.
5. Install the card.
6. Reboot the host system.

Ping to remote host is failing

Pings generated between servers are failing or there is no response from ping.

1. **Possible Cause:** Ethernet interface on either server is in the following states:
   - Administratively down. Running the Linux or VMware **ifconfig** command shows that the UP flag is not set.

- Administratively up, but link is down. Running the Linux or VMware **ifconfig** command shows that the RUNNING flag is not set.

Action: To determine link state, run the **ifconfig** command for Linux or VMware systems. For Windows systems, run **ipconfig /all** or use **Settings > Network Connections**.

Action: For the interface to send and receive packets, both the UP and RUNNING flags must be set.

Action: If pinging a server on a different network. make sure that the route to that host network or that the default gateway is correctly configured.

2. **Possible Cause:** Other link problems.

   Action: Refer to "Port link is not active" on page 10.

3. **Possible Cause:** IP address and network mask of adapter port are set incorrectly.

   Action: Verify and set IP address and network mask if necessary.

   - Linux - Run the **ifconfig** command to determine if port has proper IP address and network mask and to verify that the link is up.
   - Windows - Use Device Manager and network connection tools.

4. **Possible Cause:** Packets are not being received or stack is dropping packets at remote server due to incorrect IP address set on adapter or incorrect MTU size.

   Action: Verify if packets arrived at the remote server using the following commands:

   - Linux - Run the **tcpdump** command.
   - Windows - Run the Wireshark application.

   Action: Verify MTU size on your system and increase size if necessary. Note that MTU size set on adapter must not be more than MTU size set on attached FCoE switch. To set MTU size on the adapter, refer to the "Adapter Configuration" Chapter in the *Brocade Adapters Installation and Reference Manual*.

   Action: Verify and set IP address and network mask if necessary.

   - Linux - Run the **ifconfig** command to determine if port has proper IP address and network mask and to verify that the link is up.
   - Windows - Use Device Manager and network connection tools.

5. **Possible Cause:** If hosts with Windows operating systems do not reply to broadcast/multicast ICMP **ping** commands, this is by design. Windows systems will not reply for security reasons.

   Action: Refer to Windows KB137421 on http://support.microsoft.com/kb/137421.

Receive-side scaling disables unexpectedly

Receive-side scaling (RSS) is unexpectedly disabled on Windows Server 2008 systems.

Possible Cause: Windows hotfix KB958015 is not installed.

Action: Download and install hotfix KB958015. This hotfix is recommended.

Applications using TDI driver stop responding

Applications that use the TDI driver for network traffic may stop responding on Windows Server 2008 and Windows Vista systems.

Possible Cause: Windows hotfix KB2029048 is not installed.

Action: Download and install hotfix KB2029048. This hotfix is optional.

RSS network throughput decreases

Receive-side scaling (RSS) network throughput performance decreases on Windows Server 2008 R2 systems with more than 32 processors.

Possible Cause: Windows hotfix KB977977 is not installed.

Action: Download and install hotfix KB977977. This hotfix is recommended.

SNMP MIB browser not displaying information on VLAN-related OIDs

For Windows systems, when a large number of VLANs are created on a port, the SNMP MIB browser sometimes doesn't display the requested info for snmp_getBulk/snmp_walk/snmp_table operations on VLAN-related object identifiers (OIDs). Instead a "Failed to connect to the SNMP agent" message displays.

Possible Cause: The browser is timing out before all data is populated.

Possible Cause: Increase the default timeout value of the SNMP MIB browser to a sufficiently large value (40 seconds - 50 seconds) so that all the values populate before time-out.

Teaming errors

Ports configured as team members are in an error state and output from the BCU team --vlanquery command shows mismatching of teaming parameters. Although you can still create teams, the parameters configured for the first port (primary port) added to a team should match parameters of subsequent ports added to the team or mismatching conflict errors result.

In the following example output from the BCU **team –vlanquery** command, a conflict displays for the port associated with local area connection 6 because its PVID does not match the PVID of the primary port (local area connection 3).

```
2/0 : Local Area Connection 3 (Primary) (Active) (Linkdown)
3/1 : Local Area Connection 6 )Conflict)
Conflict Reason: Mismatching PVIDs configured for adapters
```

Note that you can still create teams even though these conflicts exist. However to avoid conflicts, make sure the following parameters match for all ports added to a team:

- Receive side scaling
- Offload parameters
- Port VLAN ID (PVID)
- MTU size
- Link speed

NOTE
For CNAs and Fabric Adapter ports configured in CNA or NIC mode, link speed is always 10 Gbps. You cannot change this parameter.

You can view and change these parameters for each port using Windows Device Manager.

1. Run **devmgmt.msc** to open the **Device Manager** window.
2. Expand **Network Adapters**.

   An instance of the adapter model should display for each installed adapter port.
3. Right-click an the adapter instance that corresponds to the port where you want to change parameters, and select **Properties**.
4. Select the **Advanced** tab.
5. Select the property and change the value as appropriate.

For more details, refer to the "Adapter Configuration" appendix in the *Brocade Adapters Installation and Reference Manual*.

VLAN creation and operation problems

VLAN creation fails with BCU command or HCM or pass-through VLAN stops working after creating with Device Manager. These problems result when VLANs are created using HCM or BCU commands and also using Device Manager. Follow these guidelines to avoid problems:

- If you need to create a single VLAN and VLANs have not been created using BCU commands or HCM, you can use Device Manager.
- If you want to configure multiple VLANs, disable the port VLAN created in Device Manager (set to 0 value), then configure VLANs using HCM or BCU. Refer to the *Brocade Adapters Administrator's Guide* for instructions.

1. **Symptom:** When using BCU commands or HCM, to create VLANs, the initial VLAN fails with an error message.

   Possible Cause: Port VLAN was created through Device Manager.

   Action: Set port VLANID to 0 in Device Manager and create VLANs using BCU commands or HCM.
2. **Symptom:** Passthru VLAN stops working.

   Possible Cause: Port VLAN was configured through Device Manager.

   Action: Set port VLANID to 0 in Device Manager.
3. **Symptom:** Right-clicking on a VLAN device in Device Manager, then selecting **Update** does not work.

   Possible Cause: The upgrade option for Brocade 10 Gig Ethernet service is not available.

   Action: Uninstall and install the service.
4. **Symptom:** No VLAN operation works except "bcu ethport --vlanlist."

   Possible Cause: Port VLAN is configured in Device Manager.

   Action: Set port VLANID to 0 in Device Manager.

5. **Symptom:** "Illegal Configuration - Remove Port VLAN" message displays when you use the **bcu vlan –list** command or list VLANs through HCM.

   Possible Cause: VLAN or Passthru VLAN was created with BCU commands or HCM and user has modified the PVID on the port with VLANs to a nonzero value.

   Action. Use Device Manager to modify the PVID on the port with VLANs to a zero (0) value.

Enabling and disabling port VLAN in Device Manager

Access the port VLAN configuration in Device Manager using the following steps.

1. Open Device Manager.
2. Expand **Network Adapters**

   An instance of the adapter model should display for each installed adapter port.
3. Right-click an adapter instance and select **Properties**.
4. Select the **Advanced** tab.
5. Select **VlanID.**
6. Set VLANID to 0 to disable or enable by setting an ID number.

Teaming or VLAN operations through HCM fail

When creating a team or VLAN through HCM on Windows 2003 systems, the operation fails and an error may result.

Symptoms: Following symptoms of this problem:

- VLAN or teaming operations fail through HCM or event 7030 occurs with the following text.

  ```
  The Brocade HCM  is marked as an interactive service. However, the system is
  configured not to allow interactive services. This service may not function
  properly.
  ```

- The HCM agent is not running in the Windows Services panel, but is running in the Task Manager.
- When creating or deleting a VLAN through HCM, the operation times out after a few minutes and a "Failed to connect to Agent on local host" or "Connection failure" message displays. Restarting the HCM Agent causes a 1053 error condition, and the agent stops in the Windows Services panel.
- Restarting the HCM Agent after creating a team through HCM results in a 1053 error.

Possible Cause: Interactive Services is disabled.

Action: Enable NoInteractRiveServices in the Windows 2003 registry. Use the following steps.

1. Run the **regedit** command.
2. Select **NoInteractiveServices** and set the value to 0.

   NoInteractiveServices is located in the following hierarchy in HKEY_LOCAL_MACHINE.

   SYSTEM\Current\ControlSet\Control\Windows

Poor network performance

Poor network performance apparent for Windows and Linux systems.

1. **Symptom:** Checksum offloads are disabled.

   Action: For Windows, verify if checksum offload parameters are enabled using the **Advanced** tab on the **Network Adapters** > **Properties** dialog box in Device Manager.

   Action: For Linux, run the **ethtool -k <interface ID>** command. If offload parameters are on, information similar to the following displays in the output.

   ```
   rx-checksumming: on
   tx-checksumming: on
   tcp segmentation offload: on
   ```

   Action: Checksum offloads should be enabled by default. If not, refer to the "Adapter Configuration" appendix in the *Brocade Adapters Installation and Reference Manual*.

2. **Symptom:** Dynamic interrupt moderation is disabled.

   Action: For Windows, verify if interrupt moderation is enabled using the **Advanced** tab on the **Network Adapters** > **Properties** dialog box in Device Manager.

   Action: For Linux, run the **ethtool -c <interface ID>** command. If interrupt moderation is enabled, information similar to the following displays in the output.

   ```
   Coalesce parameters for eth2:
   Adaptive RX: on  TX: off
   ```

   Action: Interrupt moderation should be enabled by default. If not, refer to the "Adapter Configuration" appendix in the *Brocade Adapters Installation and Reference Manual*.

3. **Symptom:** Not all eight lanes of PCIe bus are functioning.

   Action: For Linux, run the following command:

   ```
   lspci –vv –d 1657:0014
   ```

   If eight lanes are detected, information similar to the following should appear in the command output:

   ```
   Link: Supported Speed unknown, Width x8, ASPM L0s L1, Port 0
   Link: Speed 2.5Gb/s, Width x8
   ```

   Action: If eight lanes are not detected, try rebooting the system. If this does not fix the problem, contact customer support for your adapter.

Binding issues after Hyper-V enabled with teaming

Following are issues to consider when enabling Hyper-V when teams are created.

BNI driver upgraded, installed, or removed

Binding issues may result when the Brocade network intermediate (BNI) driver is upgraded, installed, or removed if there is a team created through BCU or HCM and it is enabled with Hyper-V (bound to Microsoft Hyper-V Switch Protocol).

Possible Cause: When the BNI driver is upgraded, the current configuration is saved, the old driver is removed, and the new driver installed. If a team is created and bound to Hyper-V, the virtual adapter in the team is removed when the BNI driver is removed. Therefore, the upper edge of the virtual adapter created through the Hyper-V manager for virtual managers will not have any lower edge bindings. This will lead to upper protocol and other binding issues on the system and multiple issues when reinstalling the operating system.

Action: Before upgrading, installing, or removing network driver packages, first remove the Hyper-V enablement from the team, if it is present.

Non-zero VLAN IDs

There is no restriction on creating a VLAN with non-zero ID on top of the physical adapter, using it as a base port for an existing team, and then enabling Hyper-V. However, binding issues may result.

Possible Cause: The BNI driver limits the Hyper-V enablement only to the team and not to any non-zero VLANs created on top of the Brocade's physical adapter.

Action: Enable Hyper-V only for the team created on Brocade's physical adapter and not for any virtual adapters with non-zero VLAN IDs.

Enabling Hyper-V on port that is team member

Binding issues may result if you try to enable Hyper-V on a physical port that is already part of a team.

Possible Cause: This occurs if you select a port that is a member of an existing team for Hyper-V enablement. The BNI driver cannot restrict this operation.

Action: Remove the port from the team before enabling Hyper-V.

Recovery steps

If binding issues occur when enabling Hyper-V, the following steps may work to recover the system.

- Remove the virtual adapter created through the Hyper-V manager.
- Enable Brocade's physical adapter bindings to all the upper protocols and not to the BNI driver or any other Intermediate driver.
- Reboot the server.
- Assign an IP address to the physical adapter and ping some peer in the network. If this works, then the user can assume that the system has recovered

FCoE and Fibre Channel problems

This section provides resolution of the following:

- Fibre Channel problems on HBAs and Fabric Adapter ports configured in HBA mode.
- FCoE problems on CNAs and Fabric Adapter ports configured in CNA mode.

Loss of sync and loss of signal errors in port statistics

If the port is having loss of synchronization and signal errors, refer to the following descriptions of possible causes and recommended actions to help resolve the problem. Learn more about displaying port statistics in "Port statistics" on page 82.

Possible Cause: Possible physical link problem.

Action: Check authentication settings on the switch and adapter. For the switch, execute the **authutil –show Fabric** Fabric OS command. For the adapter, execute the BCU **auth –show** command (refer to "Authentication settings" on page 105).

Action: Use the BCU **auth –show <port>** command on the adapter and Fabric OS **authutil –show** command on the switch.

Action: Check the shared secret configuration on the attached switch and on the adapter. For the switch, execute the **secAuthSecret** Fabric OS command. For the adapter, execute the **auth –-secret** BCU command. Refer to "Authentication settings" on page 105 for details on using the auth-secret command.

Fabric authentication failures

If failures in the authentication process between the adapter in host system and the connected switch occur, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Authenticating configuration is incorrect.

Action: Check authentication settings on the switch and adapter. For the switch, execute the **authutil –show** Fabric OS command. For the adapter, execute the BCU **auth –show** command (refer to "Authentication settings" on page 105).

Action: Check the shared secret configuration on the attached switch and adapter. For the switch, execute the **secAuthSecret Fabric** OS command. For the adapter, execute the **auth –-secret** BCU command. Refer to "Authentication settings" on page 105 for details on using the **auth-secret** command.

Adapter is not showing in the fabric

If the adapter does not appear as a Fibre Channel device in the fabric, refer to the following descriptions of the possible cause and recommended action to help resolve the problem.

Possible Cause: There is a problem in the fabric or a protocol issue between the adapter and a fabric.

Action: Check the fabric statistics. Refer to "Fabric statistics" on page 76 for methods to display fabric statistics for the adapter.

- If counts for FLOGI sent and FLOGI accept fabric statistics do not match, suspect fabric problem or protocol issue between adapter and fabric.
- If fabric offline counts increase and fabric maintenance is not occurring, this may indicate a serious fabric problem. Refer to your switch troubleshooting guide to isolate and resolve the problem.

Virtual devices not listed in name server

If virtual devices are not listed in the fabric's name server, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Causes:

- Problem in the fabric or a protocol issue between the adapter and fabric.
- NPIV is not supported or is disabled on the switch.

Action: Check virtual port statistics, such as FDISC sent, FDISC accept, and No NPIV support statistics. Refer to "Virtual port statistics" on page 87 for methods to display virtual port statistics.

Adapter not registering with the name server or cannot access storage

If the adapter is not registering with the name server or cannot access storage, refer to the following descriptions of possible causes and recommended actions to help solve the problem.

1. **Possible Cause:** Adapter cannot log in to the name server.

   Action: Display logical port statistics (refer to "Logical port statistics" on page 80 for details on displaying these statistics). Check for increasing name server port login (NS PLOGI) error rejects and unknown name server port login response (NS login unknown rsp). These errors mean that the adapter most likely cannot log in to the name server.

2. **Possible Cause:** Adapter has a problem registering with the name server.

   Action: Display logical port statistics (refer to "Logical port statistics" on page 80 for details on displaying these statistics). Check for increasing errors of the following types. These indicate that the adapter has a problem registering with the name server:

   - Name server register symbolic port name identifier (NS RSPN_ID) errors.
   - Name server register symbolic port name identifier response (NS RFT_ID rsp) errors.
   - Name server register symbolic port name identifier response rejects (NS RFT_ID rejects).

3. **Possible Cause:** Adapter has a problem querying the name server for available storage.

   Action: Display logical port statistics (refer to "Logical port statistics" on page 80 for details on displaying these statistics). Check for increasing name server "get all port ID response" (NS GID_FT rsp), rejects (NS_GID FT rejects), or unknown responses (NS_GID FT unknown rsp). This indicates that the adapter has a problem querying the name server for available storage.

FCoE link is down

NOTE
This issue applies to CNAs and Fabric Adapter ports configured in CNA mode only.

The FCoE link is down between the adapter and switch.

1. **Possible Cause:** The FCoE link is not administratively enabled.

   Action: Determine if the link is enabled by entering the BCU **port –list** command. If the port is administratively disabled, the **"port state"** field will show **Disabled**.

   Action: Enable the port by entering the BCU **port –enable <port_id>** command.

2. **Possible Cause:** The FCoE license may not be installed on the connected switch.

   Action: Execute the Fabric OS **licenseshow** command on the connected switch to determine if the license is installed. Install license if not installed. For more information about Fabric OS commands and QoS support, refer to the *Fabric OS Administrator's Guide*.

3. **Possible Cause:** The DCB link is not enabled on the adapter.

   Action: Verify that the DCB status using the BCU **port –list** command is displayed as "DCB Linkup". If "Linkdown" or "Linkup" displays, refer to "DCB is not enabled" on page 45.

4. **Possible Cause:** The VLAN to which the FCoE switch front-end port belongs is not FCF-capable.

   Action: Verify if VLAN on front-end port is FCF-capable using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric-OS Command Reference Manual* for more information.

   Action: Set the VLAN as FCF-capable using the appropriate Fabric OS commands on the attached FCoE switch. Refer to the *Fabric-OS Command Reference Manual* for more information.

5. **Possible Cause:** The FC-MAP on the FCoE switch is not set for a VLAN with FCF capability.

   Action: Verify if the FC-MAP on the switch is set for a VLAN with FCF capability using appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for more information.

   Action: Set the FC-MAP for a VLAN with FCF capability using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for more information.

6. **Possible Cause:** The FCoE Login group is not created on the FCoE switch, not allowing all VF-Ports to be part of the login group.

   Action: Verify if FCoE Login group is created on switch using the appropriate Fabric OS command. Refer to the *Fabric OS Command Reference Manual* for information.

   Action: Create an FCoE login group on the switch using the appropriate Fabric OS command.

7. **Possible Cause:** PFC (priority flow control), DCB Map, and FCoE Map is not configured correctly on the FCoE switch.

   Action: Refer to "DCB is not enabled" on page 45.

8. **Possible Cause:** For IBM blade systems, the BladeCenter Open Fabric Manager (BOFM) support in adapter option ROM expects non-zero values for PWWN and NWWN for the FCoE port. If any values are zero, the link will not come up and port status will display **Linkdown**.

Action: Verify if the PWWN or NWWN has a zero value using one of these methods:

- Windows system log or Linux /var/log/messages file displays a port error indicating a zero PWWN or NWWN.
- Output from **bcu port –query <port_id>** command for the port shows zero value for PWWN or NWWN.
- Advanced Management Module (AMM) Open Fabric Manager (OFM) status page displays an error status for the corresponding port of the blade.

If values are zero, use BOFM to configure non-zero values for the PWWN and NWWN.

I/O problem on connected FCoE device

NOTE
This issue applies to CNAs and Fabric Adapter ports configured in CNA mode only.

There is an I/O problem on a connected FCoE device.

1. **Possible Cause:** Link between the adapter and switch is down.

   Action: Refer to "FCoE link is down" on page 43.

   Action: Refer to "DCB is not enabled" on page 45.

2. **Possible Cause:** PFC (priority flow control), DCB Map, and FCoE Map is not configured correctly on the FCoE switch.

   Action: Verify configuration using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for information.

   Action: Configure PFC using the appropriate Fabric OS command on the attached switch while in switch configuration mode.

3. **Possible Cause:** Zoning is configured incorrectly on FCoE switch.

   Action: Verify zoning configuration on the attached switch using the appropriate Fabric OS command. Refer to the *Fabric OS Command Reference Manual* for more information.

I/Os are not failing over immediately on path failure in MPIO setup

When multipath I/O (MPIO) is enabled and input/output operations are not failing over immediately when a path failure occurs, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Improper driver mpiomode setting.

Action: Execute the **port –query <port_id>** BCU command and ensure fcpim MPIO mode is enabled (which implies zero Path TOV values) or that fcpim MPIO mode is disabled with the expected "Path TOV" settings (default is 30 seconds).

Disk I/O requests cause low throughput and high latency on Linux

If a high number of I/O requests is causing low throughput and high latency on Linux systems, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: The maximum input/output operations per second are too low on Linux hosts.

Action: Refer to "Linux tuning" on page 113 for suggestions to optimize adapter performance in Linux systems.

Disk I/O requests cause low throughput and high latency on VMware

If a high number of I/O requests is causing low throughput and high latency on VMware systems, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: The maximum input/output operations per second are too low on VMware hosts.

Action: Refer to "VMware tuning" on page 116 for suggestions to optimize adapter performance in VMware systems.

DCB network problems

NOTE
This issue applies to CNAs and Fabric Adapter ports configured in CNA mode only.

This section provides information to resolve problems of adapter operation on the Data Center Bridging (DCB) network. For additional information on troubleshooting problems on mezzanine card or expansion card adapters, refer to "Troubleshooting mezzanine card problems" on page 55.

DCB is not enabled

The DCB state does not show "DCB Linkup" when you run the BCU **port –query** command.

1. **Possible Cause:** The link between the adapter port and switch is down.

   Action: Run the **dcb –query** command for the port to gain a better understanding of LLDP attributes, DCB maps, and priority tables configured for the port. Also check the error reason code for the DCB link failure. The error reason code will tell you why the DCB is not enabled or active. If the error reason is "Physical Link down," refer to "Port link is not active" on page 10 and "Verifying Fibre Channel and DCB links (stand-up adapters)" on page 50.

2. **Possible Cause:** Adapter did not receive DCB configuration or received invalid DCB configuration from the FCoE switch.

   Action: Run the BCU **dcb –query** command for the port to gain a better understanding of LLDP attributes and DCB configuration (such as DCB maps and priority tables) configured for the port. Also check for the error reason code for the DCB link failure. The reason code will tell you why the DCB is not enabled or active. Change or fix the DCB configuration at the switch appropriately based on the displayed error reason code.

Action: Check FCoE switch configuration using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for information. Change configuration as necessary using appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for information.

3. **Possible Cause:** The front-end Ethernet port on the FCoE switch is not configured as "switchport" or is not set to converged mode.

   Action: Use the appropriate Fabric OS command on the attached switch to display information about the VLAN interface. Refer to the *Fabric OS Command Reference Manual* for information.

   Action: Configure the FCoE port as a "switchport" using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for information.

   Action: Configure the FCoE port to converged mode using the appropriate Fabric OS command on the attached switch.

HCM and HCM Agent problems

This section provides information to help resolve problems with HCM installation and operation.

Failed to connect to agent on host... error when using HCM

An "Adapter failed to connect to agent on host..." message indicates that the client application cannot connect to the HCM agent listening on the configured port (normally TCP port 34568). Refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** If the hcmagent process exited in VMware ESX 3.5 or 4.x, the HCM Agent may be configured to forward events to a remote Syslog host, but the outgoing UDP port 514 is blocked by the ESX firewall.

   Action: Perform the following steps.

   a. Run the following command to open port 514.

      ```
      esxcfg-firewall -o 514,udp,out,syslog
      ```

   b. Start the agent using the following command.

      ```
      hcmagentservice start
      ```

2. **Other Possible Causes:**

   - The HCM Agent is not running.
   - The HCM Agent is not accepting connections on the expected port.
   - The HCM Agent is not listening on the expected port.
   - Communication between the client and agent is blocked by a firewall preventing access to the port (usually only a consideration for remote HCM management).

Action: For Linux, Solaris, and VMware systems, perform the following steps to help isolate the problem:

a. Verify that the agent is running by executing the appropriate **status** command for your operating system as described in the "Software Installation" chapter in the *Brocade Adapters Installation and Reference Manual* under "HCM Agent Operations."

b. If you receive a message that the hcmagent is stopped, restarting the agent should resolve the problem. To restart, use the appropriate **start** command for your operating system which is also described in the "Software Installation" chapter in the *Brocade Adapters Installation and Reference Manual* under "HCM Agent Operations."

c. Note that one command described in the manual restarts the agent, but the agent will not restart if the system reboots or the agent stops unexpectedly. Another command restarts the agent, but the agent will restart if the system reboots.

d. Confirm the HCM Agent is responding to requests using the expected user password. Execute the following command to connect to the HCM Agent and force it to collect the adapter driver supportsave data.

NOTE
This command is a single line. The localhost can be replaced with a different IP address.

```
wget --no-check-certificate
https://admin:password@localhost:34568/JSONRPCServiceApp/
SupportSaveController.do
```

If successful, the file SupportSaveController.do (actually a zip format file) will contain the data from the HCM Agent.

e. If you are managing a VMware host system through HCM from a remote system, the host's firewall may be blocking TCP/IP port 34568, which allows agent communication with HCM.

Use the following command to open port 34568.

```
/usr/sbin/esxcfg-firewall-o 34568,tcp,out,https
```

Use Windows Firewall and Advanced Service (WFAS) to open port 34568.

NOTE
You can change the default communication port (34568) for the agent using procedures in the "Software Installation" chapter in the *Brocade Adapters Installation and Reference Manual* under "HCM Agent Operations."

f. If HCM is still unable to connect to the HCM Agent after using the preceding steps, collect the following data and send to your Support representative for analysis:

- Data collected from the previous step in SupportSaveController.do.
- Data from the HCM application SupportSave feature. Select **Tools** > **SupportSave** to generate a supportsave file. The data file name and location displays when the SupportSave feature runs.
- Adapter agent files on the adapter host (where the HCM Agent is installed). Collect these files using the command **tar cvfz hbafiles.tgz /opt/hba**. Output collects to hbafiles.tgz.

- Data collected on the adapter host from the bfa_supportsave feature using the **bfa_supportsave** command. Output collects to a file and location specified when the SupportSave feature runs.

Action: For Windows systems, perform the following steps on to help isolate the problem:

a. Verify that the agent is running by executing the appropriate **status** command for your operating system described in the *Brocade Adapters Installation and Reference Manual*. Refer to the section on modifying HCM Agent operation.

b. If you receive a message that the hcmagent is stopped, restarting the agent should resolve the problem. To restart, use the appropriate **start** command for your operating system which is also described in the *Brocade Adapters Installation and Reference Manual*.

Note that one command described in the *Brocade Adapters Installation and Reference Manual* restarts the agent, but the agent will not restart if the system reboots or the agent stops unexpectedly. Another command restarts the agent, but the agent will restart if the system reboots.

a. If the HCM Agent starts, verify which TCP port the agent is listening on by executing the following command at the Windows command prompt.

```
netstat -nao | findstr 34568
```

Output similar to the following should display.

```
TCP    0.0.0.0:34568          0.0.0.0:0              LISTENING       1960
```

The value 1960 in the last column is the process identifier for the Windows process listening on the TCP port. Note that this identifier may be different on your system.

b. Enter the following command to confirm that the process identifier bound to TCP port 34568 is for the hcm.exe process.

```
tasklist /svc | findstr 1960
```

The following should display if the identifier from step a is bound to TCP port 34568.

```
    hcmagent.exe                 1960 hcmagent
```

c. If you are managing a Windows 2008 host system through HCM from a remote system, the host's firewall may be blocking TCP/IP port 34568.

NOTE
Use Windows Firewall and Advanced Service (WFAS) to open port 34568.

NOTE
You can change the default communication port (34568) for the agent using procedures in the *Brocade Adapters Installation and Reference Manual*. Refer to the section on modifying HCM Agent operation.

d. If the HCM Agent is running and listening on port 34568 and there are no firewall issues (as explained in step c), but you get the same "Failed to connect to agent on host..." error when using HCM, collect the following data. Send the following data to your support representative for analysis:

- Copies of output from the commands in step a and step b.

- Files from the output directory created after you execute the support save feature. To collect these files, execute the BCU **bfa_supportsave** command. Support data is collected to a file in your system's tmp directory by default. For more information on using the Support Save feature, refer to "Support Save" on page 61.
- Support data from the HCM application SupportSave feature.
- Build information for the HCM application. Select **Help > About** in HCM to display the version, build identification, and build date.

To use the HCM SupportSave feature, select **Tools > Support Save** in HCM to generate a supportsave file. If HCM cannot connect to the agent, a message displays an error (Support Save could not be collected) and explains that only a basic collection is possible. Messages also display that provide the location of the zip file created.

By default, a zip file is created in the following location.

```
<user home>\HCM\data\localhost\supportsave
```

The zip file will have a name similar to the following.

```
SupportSave_Advanced_2008723_0_50_57.zip
```

HCM Agent service cannot start

When starting the HCM Agent from the command line on Windows 2003 R2 SP2 systems, an error displays that "The program cannot be run."

Possible Cause: Visual Studio 2005 SP1 (or later) Redistributable package is not installed.

Action: Install the Visual Studio 2005 SP1 (or later) Redistributable package.

HCM Agent not auto starting if 3.0 driver updated with 2.3 HCM

HCM Agent will not start automatically after system reboot if upgrading with 3.0 drivers and 2.3 HCM is installed.

Possible Cause: Driver update is setting the HCM Agent to manual start.

Action: Enter the following command at the command line:

```
sc config hcmagent start= auto
```

Unable to completely uninstall HCM

Removing HCM using Windows **Add or Remove Programs** causes "Unable to completely uninstall application" error.

Possible Cause: HCM was installed on a host system through the HCM Agent on server system using the web browser.

Action: Use one of the following methods to remove HCM from the host system:

Method 1

1. Enter the following at the command prompt:

   ```
   Javaws -viewer
   ```

   The **Java Cache Viewer** screen displays.

2. Select **Host Connectivity Manager**, right click, and then select **Delete** from the menu.

Method 2

1. Enter the following at the command prompt:

```
Javaws -uninstall
```

   This installs all applications in the Java cache.

Time on HCM screens does not match system time

The time display on HCM screens, such as on the main HCM window and statistics dialog boxes, show time relative to GMT instead of the host system time zone. This is a problem on Windows Server 2003 systems.

Possible Cause: Java virtual machine does not get correct time zone information from the windows registry of the local system and defaults to a time zone relative to the GMT. Possibly the Microsoft timezone.exe tool was launched, which may cause Java applications to return incorrect time and date information.

Action: Use the Time Zone Editor (tzedit.exe utility) to change the time zone settings on a single system. Download this tool from the Microsoft download site at http://www.microsoft.com/downloads.

Follow these recommendations:

- You must have local administrative credentials to change time zone registry information with the Time Zone Editor.
- The Time Zone Editor does not provide the capabilities to add the Dynamic DSTregistry subkeys.
- Obtain the list of time zones that have changed, together with their DST start dates and end dates. Use the information in the following article located at http://support.microsoft.com/kb/981128.

  "A hotfix is available to update the Daylight Saving Time for the "(UTC-04:00) Asuncion", "(UTC+12:00) Fiji" and "(UTC-04:00) Santiago" time zone for Windows Operating Systems."

Verifying Fibre Channel and DCB links (stand-up adapters)

Check for link problems on stand-up adapters by observing LED operation for adapter ports. LED operation other than expected or LEDs may indicate link problems. For example, all LEDs flashing amber for a port indicates that an invalid non-Brocade SFP may be installed. For details on adapter LED operation, refer to the "LED Operation" section for your adapter in the *Brocade Adapters Installation and Reference Manual*. If LEDs do not illuminate to indicate an active link, use appropriate Fabric OS and adapter diagnostic commands and HCM options in Table 3 on page 51. For additional diagnostics commands, refer to Chapter 3, "Tools for Collecting Data" for HCM and BCU commands and the *Fabric OS Administrator's Guide* for Fabric OS commands.

NOTE
Also verify LED operation on a switch port that is connected to an adapter port. Refer to the switch hardware reference manual to analyze LED meaning.

Common link problems can be caused by the following:

- Damaged cables. (Note that damaged cables can also cause errors and invalid data on links.)
- Cables that are not rated or compatible with adapter port speeds. Refer to cable specifications in the *Brocade Adapters Installation and Reference Manual*.
- Faulty switch or adapter SFPs. Verify if an SFP is the problem by connecting a different link to the adapter port or, if convenient, replace the cable with a cable of known quality. If the errors or invalid data on the link still indicate a cable problem, the SFP may be faulty. Try replacing the SFP.
- SFP issues on the adapter or switch. For example, the SFP may not be compatible with the adapter, but is compatible with the switch, or vice versa. SCSI retries and time-outs determine communication between the adapter and storage. Dropped packets cause time-outs, and packets can drop because of SFP issues. Run the BCU **port -stats** command to display port statistics, and look for errors and dropped frames.

Table 3 lists HCM options and BCU commands, as well as Fabric OS commands that you can use to determine link status.

TABLE 3 Tools to determine link status

Application	Tool	References
HCM	• Port Statistics • Loopback and PCI loopback test • Fibre Channel ping, echo, and trace route tests • Link Beaconing • Port Properties • SFP information	*Chapter 3, "Tools for Collecting Data"*
BCU	• **fcdiag** and **diag** commands. • Port commands, such as **port –stats**. **port –list**, and **port –query.**	*Chapter 3, "Tools for Collecting Data"*
Switch Fabric OS	• switchShow • portShow • portStatsShow • portErrShow • fcpProbeShow • fPortTest	• *Chapter 3, "Tools for Collecting Data"* • *Fabric OS Administrator's Guide* • *Fabric OS Troubleshooting* and *Diagnostics Guide*

Adapter driver installation verification

Problems with adapter operation may be due to improper hardware or software installation, incompatibility between the adapter and your host system, unsupported SFPs installed on the adapter, improper cable connected to the fabric, or the adapter not operating within specifications. Determine if problems may exist because of these factors by reviewing your installation with information in the *Brocade Adapters Installation and Reference Manual* listed in Table 4.

TABLE 4 Installation and Reference Manual references

Information	Chapter
Hardware and software compatibility information.	Product Overview
Software installation packages supported by host operating system and platforms.	Product Overview
Hardware and software installation instructions.	Installation
Product specifications.	Specifications

Adapter driver packages from Brocade contain the current driver, firmware, and HCM Agent for specific operating systems. Make sure that the correct package is installed for your operating system. Refer to the Product Overview chapter in the *Brocade Adapters Installation and Reference Manual*.

An out-of-date driver may cause the following problems:

- Storage devices and targets not being discovered by the device manager or appearing incorrectly in the host's device manager.
- Improper or erratic behavior of HCM (installed driver package may not support HCM version).
- Host operating system not recognizing adapter installation.
- Operating system errors (blue screen).

NOTE
If a driver is not installed, try re-installing the driver or re-installing the adapter hardware and then the driver.

You can use HCM and tools available through your host's operating system to obtain information such as driver name, driver version, and adapter PWWNs.

Confirming driver package installation with HCM

Use the following steps to display the adapter PWWN, driver name and version, firmware name and version, and the BIOS version currently in operation.

1. Launch HCM.
2. Select the adapter in the device tree.
3. Select the **Properties** tab in the right pane to display the **Properties** dialog box.

   The dialog box displays adapter properties.

Confirming driver package installation in Windows systems

Use the Device Manager to determine driver installation. Verify if the driver is installed and Windows is recognizing the adapter using the following steps.

1. Open the Device Manager.
   - For CNAs, HBAs, and Fabric Adapters, when you expand the list of **SCSI and RAID controllers** or **Storage controllers** an instance of the adapter model should display for adapter port installed.

- For CNAs and Fabric Adapter ports configured in CNA or NIC mode, when you expand **Network adapters**, an instance of **Brocade 10G Ethernet Adapter** should also display for each port installed.

For example, if two two-port CNAs (total of four ports) are installed, four instances of the adapter model display (two under **SCSI and RAID controllers** and two under **Network adapters**). As another example, if only one port on a Fabric Adapter is configured in CNA or NIC mode, two instances of the adapter model display (one under **SCSI and RAID controllers** and one under **Network adapters).**

If instances of your adapter model do not display, but generic instances flagged with yellow question marks *do* display under **Other Devices**, the driver is not installed. For example, **Fibre Channel Controller** may display as a generic instance for an HBA or Fabric Adapter port configured in HBA mode.

2. Right-click the Brocade adapter model where you are installing the driver.
3. Select **Properties** to display the **Properties** dialog box.
4. Click the **Driver** tab to display the driver date and version. Click **Driver Details** for more information.

NOTE
If driver is not installed, try re-installing the driver or re-installing the adapter hardware and then the driver.

Confirming driver package installation in Linux systems

Verify if the adapter driver installed successfully using the following commands:

- **# rpm -qa|grep -i bfa**

  This command prints the names of the Brocade adapter storage driver package (bfa) if installed.

- **# rpm -qa|grep -i bna**

  This command prints the names of the Brocade adapter network driver package (bfa) if installed.

- **# lspci**

  This utility displays information about all PCI buses in the system and all devices connected to them. **Fibre Channel: Brocade Communications Systems, Inc.** displays for an HBA or Fabric Adapter port configured in HBA mode. **Fibre Channel: Brocade Communications Systems, Inc.** and **Ethernet Controller** display for a CNA or Fabric Adapter port configured in CNA or NIC mode if driver packages have correctly loaded.

- **# lsmod**

  This command displays information about all loaded modules. If **bfa** appears in the list, the storage driver is loaded to the system. If **bna** appears in the list, the network driver is loaded to the system.

- **# dmesg**

  This command prints kernel boot messages. Entries for **bfa** (storage driver) and **bna** (network driver) should display to indicate driver activity if the hardware and driver are installed successfully.

- These commands display the location of the driver modules if loaded to the system:
  - The following command displays the storage driver module location. The module will have a **bfa** prefix.

    ```
    # modprobe -l bfa
    ```

  - The following command displays the network driver module location. The module will have a **bfa** prefix.

    ```
    # modprobe -l bna
    ```

Confirming driver package installation in Solaris systems

Verify if the adapter driver installed successfully using the following commands:

NOTE
Brocade 804 and 1007 adapters are not supported on Solaris systems so these commands do not apply to those adapters.

- **pkgchk -nv bfa**

  This checks for and lists the installed adapter storage driver package files.

- **pkginfo -l bfa**

  This displays details about installed Brocade storage (bfa) adapter drivers. Look for information to display like in the following example. Note that the VERSION may be different, depending on the driver version you installed. The ARCH and DESC information may also be different, depending on your host system platform. If the adapter driver package is installed, bfa_pkg should display with a “completely installed” status.

  Storage driver (bfa)

```
PKGINST: bfa
      NAME:  Brocade Fibre Channel Adapter Driver
  CATEGORY:  system
      ARCH:  sparc&i386
   VERSION:  alpha_bld31_20080502_1205
   BASEDIR:  /
    VENDOR:  Brocade
      DESC:  32 bit & 64 bit Device driver for Brocade Fibre Channel
adapters
    PSTAMP:  20080115150824
  INSTDATE:  May 02 2008 18:22
   HOTLINE:  Please contact your local service provider
    STATUS:  completely installed
```

Confirming driver package installation in VMware systems

Verify if the adapter driver installed successfully using the following commands:

- **esxcfg-module -l**

  This lists installed driver names, R/O and R/W addresses, and whether the ID is loaded. For storage drivers, verify that an entry for **bfa** exists and that the ID loaded. For network drivers, verify that an entry for bna exists and that the ID loaded.

- **cat /proc/vmware/version**

  This displays the latest versions of installed drivers. For storage drivers look for a **bfa** entry and related build number. For network drivers, look for a **bna** entry and related build number.

- **rpm -qa|grep -i bfa**

  This command prints the names of the Brocade adapter storage driver package (bfa) if installed.

- **rpm -qa|grep -i bna**

  This command prints the names of the Brocade adapter network driver package (bna) if installed.

- **lspci**

  This utility displays information about all PCI buses in the system and all devices connected to them. **Brocade Communications Fibre Channel** displays for an HBA or Fabric Adapter port configured in HBA mode. **Brocade Communications Fibre Channel** and **Ethernet Controller** display for a CNA or Fabric Adapter port configured in CNA or NIC mode if driver packages have correctly loaded.

Troubleshooting mezzanine card problems

As mezzanine or expansion card adapters are installed in blade servers as part of a blade system enclosure, problems may occur for different reasons than when adapters are installed in standard host systems. This section outlines some general methods for isolating causes of problems with card operation. For more information, please see troubleshooting and maintenance information published for your specific blade server, server blade, and blade system enclosure. Also, refer to the support location on the manufacturer's website for your blade server and blade system enclosure.

If problems exist with adapter operation on a blade server, verify the following:

- The blade server is turned on.
- The adapter is installed in the appropriate connector on the blade server. On some blade servers, connectors may only support a specific adapter type. Refer to your blade sever documentation for help.
- The blade system enclosure is configured for adapter operation. Refer to your blade system enclosure and documentation for blade system enclosure components for help.
- The blade server on which the adapter is installed is correctly configured for adapter operation and is correctly installed in the blade system enclosure. Refer to your blade server and blade system enclosure documentation for help.
- All modules or blades in that support adapter operation are installed in the appropriate enclosure bays and correctly configured. Refer to the documentation for your blade system enclosure for help.
- You are using the latest device drivers, firmware, and BIOS for the blade server and other components in the blade system enclosure that support adapter operation.

Additional references for isolating problems

Refer to the following publications and to chapters in this manual for gathering information to further isolate and resolve adapter problems.

- Chapter 3, "Tools for Collecting Data" in this manual

  Contains procedures to perform adapter diagnostics, display adapter statistics and display event logs, and collect data for troubleshooting using BCU commands, HCM options, Fabric OS commands, and your host system commands.

- *Fabric OS Administrator's Guide*

  Provides detailed information on features available on Brocade storage area network (SAN) products, and how to configure and administer these products

- *Fabric OS Command Reference Manual.*

  Provides detailed descriptions of command line interface commands to help system administrators and technicians operate, maintain, and troubleshoot Brocade SAN products.

- *Fabric OS Troubleshooting and Diagnostic Guide.*

  Provides help with isolating problems in other Brocade SAN components.

- Your host's operating system documentation and help system.

  Provides details on commands for gathering information and isolating problems.

Chapter

3

Tools for Collecting Data

In this chapter

- For detailed information 58
- Data to provide technical support 58
- Data collection using host system commands 59
- Data collection using BCU commands and HCM 61
- Data collection using Fabric OS commands (Brocade switches only) 66
- Adapter event messages 67
- Logs 69
- Statistics 73
- Diagnostics 89
- Collecting BIOS data 97
- Collecting LLDP data (CNA) 97
- Collecting SFP data (stand-up adapters) 98
- Collecting port data 99
- FCP-IM I/O profiling 104
- Collecting teaming information (CNA or NIC) 104
- Authentication settings 105
- PHY module data 106
- QoS settings (HBA) 106
- Target rate limiting settings (HBA) 107
- Persistent binding 108
- Adapter properties 109
- Adapter queries 111

For detailed information

This chapter provides basic instruction on tools useful for gathering information to isolate adapterproblems. For more detailed information on using these tools, refer to the *Brocade Adapters Administrator's Guide.*

The following chapters in this guide cover adapter HCM and BCU monitoring and diagnostics tools:

- Monitoring
- Diagnostics
- Brocade Command Utility (BCU)

- *Fabric OS Troubleshooting and Diagnostics Guide*

  This guide provides detailed information on collecting troubleshooting information and isolating general SAN problems between the Brocade switch, host systems, and storage systems.

- *Fabric OS Command Reference Manual*

  Fabric OS diagnostic and monitoring commands for Brocade switches.

- Your host system's operating system user and administrator's guides.

  Host system diagnostics, logs, and system monitoring tools.

- Your blade system enclosure and blade server troubleshooting publications. Use these to troubleshoot mezzanine or expansion card adapter problems.

Data to provide technical support

When problems occur requiring support assistance, provide a detailed description of the problem, as well as output collected from the following HCM and BCU tools:

- Support Save
- Diagnostics
- Port logs
- Port statistics and properties
- Adapter properties
- Host operating system error logs

Data collection using host system commands

Table 5 describes commands common to each supported operating system that you can use to gather information for troubleshooting problems. For details on these commands, refer to your system's online help and documentation.

NOTE
Output from all of these commands is captured using the Support Save feature.

TABLE 5 Host system data collection commands

Task	Linux	Windows	VMware	Solaris[1]
Listing PCI devices	lspci -vv	In Windows registry location HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Enum\PCI devcon find pci*	lspci -vv, esxcfg-info -w	prtdiag -v, prtconf -pv
Listing installed HW details	lsdev	msinfo32.exe Click the plus sign(+) next to Components to view hardware details.	esxcfg-info -a	prtdiag -v, prtconf -pv
Displaying process information	ps -efl, top	Windows Task Manager, tasklist.exe	ps -efl, top	ps -efl, top
Displaying memory usage	top, vmstat -m	Windows Task Manager, tasklist.exe	top, vmstat -m	vmstat -s
Monitoring performance	iostat, vmstat, sar	Windows Task Manager, perfmon.exe	vmstat, VM Performance: esxtop [first type 'v', 'e' then enter vm# in the list down], Disk Performance: esxtop [type 'v' then 'd'].	iostat -nx 1 5, vmstat, mpstat, sar
Listing driver modules	lsmod	driverquery	esxcfg-module -l	modinfo
Checking for Brocade Fibre Channel adapter (BFA) driver module	lsmod | grep bfa	driverquery /v | findstr bfad	esxcfg-module -l | grep bfa	modinfo | grep bfa
Checking for Brocade network (BNA) driver module	lsmod | grep bna	driverquery /v | findstr bnad	esxcfg-module -l | grep bfa	NA
Displaying driver information	• Use lsmod command for general driver information. • Use ethtool options to query network driver information and settings.	On Device Manager Right-click storage controller or network adapter instances, select **Properties**, then select **Driver** tab.	• For general driver information use esxcfg-module. • For network driver information, use esxcfg-nics.	Use modinfo options for bna or bfa driver.

TABLE 5 Host system data collection commands (continued)

Task	Linux	Windows	VMware	Solaris[1]
Locating system log messages **NOTE:** For more information, refer to "Host system logs" on page 69.	dmesg, /var/log/message*	System Category in Windows Event Viewer (eventvwr.exe)	/var/log/vmkernel* /var/log/vmkwarning*/proc /vmware/log /var/log/message*	dmesg, /var/adm/message*
Showing operating system distribution info	(SuSE) cat /etc/SuSE-release, (RedHat) cat /etc/redhat-release	systeminfo.exe	cat /etc/vmware-release	uname -a, cat /etc/release
Locating BFA configuration file	/etc/bfa.conf	Windows Registry (HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\bfad\Parameters\Device), adapter Flash	/etc/bfa.conf	/kernel/drv/bfa.conf
Locating BFA device file	/dev/bfa*	Windows Registry (HKEY_LOCAL_MACHINE \HARDWARE\DEVICEMAP\Scsi\Scsi Port x)	/opt/brocade/adapter/bfa/bfa.conf	• (Release 1.0) - /devices/pci*/pci*/fibre-channel@0:devctl, • (Release 1.1 and later) - /devices/pci*/pci*/bfa@0:devctl
Locating BNA device file	/dev/bna*	Windows Registry (HKEY_LOCAL_MACHINE \HARDWARE\DEVICEMAP\Scsi\Scsi Port x)	/dev/bna*	• (Release 1.0) - /devices/pci*/pci*/fibre-channel@0:devctl, • (Release 1.1 and later) - /devices/pci*/pci*/bfa@0:devctl
Verifying network interface parameters, such as link status, IP address, and subnet mask.	ifconfig	ipconfig Settings > Network Connections	ifconfig	N/A
Ethernet statistics	ethtool -S <interface_name>	netstat	ethtool -S <interface_name>	N/A
Ethernet link status	ethtool interface_name>	netstat	esxcfg-nics -l	N/A

1. Solaris does not support Brocade 804 and 1007 adapters so Solaris commands do not apply to these adapters.

Data collection using BCU commands and HCM

You can collect a variety of information on installed Brocade adapters, such as firmware version installed, operational status, port speed, WWN, PCI data, configuration data, flash status, and other details for troubleshooting using BCU commands, HCM menu options, Management applications, such as Network Advisor, and host operating system commands.

NOTE
For Windows systems only, launch BCU and display the BCU command prompt through the BCU desktop shortcut. Launching BCU using other methods is not recommended and may result in display of inconsistent information.

Support Save

The Support Save feature is an important tool for collecting debug information from the driver, internal libraries, and firmware. You can save this information to the local file system and send to support personnel for further investigation. Use one of the following options to launch this feature:

- For HCM, launch Support Save through the **Tools** menu.
- For management applications, such as Network Advisor, use the **Technical SupportSave** dialog box.
- For BCU on Windows systems, launch BCU using the Brocade BCU desktop shortcut and enter **bfa_supportsave** at the BCU command prompt (BCU>).
- For BCU on non-Windows systems, enter **bfa_supportsave** at your operating system prompt (direct mode) or at the BCU> command prompt using the BCU shell mode. For details on using BCU commands, refer to the *Brocade Adapters Administrator's Guide*.
- Through your internet browser (Internet Explorer 6 or later or Firefox 2.0 or later), you can collect bfa_supportsave output if you do not have root access, do not have access to file transfer methods such as FTP and SCP, or do not have access to the Host Connectivity Manager (HCM).
- A bfa_supportsave collection can also occur automatically for a port crash event.

Launching Support Save through BCU, HCM, and during a port crash event collects the following information:

- Adapter model and serial number
- Adapter firmware version
- Host model and hardware revision
- All support information
- Adapter configuration data
- All operating system and adapter information needed to diagnose field issues
- Information about all adapters in the system
- Firmware and driver traces
- Syslog message logs
- Windows System Event log .evt file
- HCM-related engineering logs
- Events

- Adapter configuration data
- Environment information
- Data .xml file
- Vital CPU, memory, network resources
- HCM (logs, configuration)
- Driver logs
- Install logs
- Core files
- Details on the Ethernet interface, including IP address and mask (CNAs and Fabric Adapter ports configured in CNA or NIC mode)
- Status and states of all adapter ports, including the Ethernet, FCoE, and DBA ports (CNAs and Fabric Adapter ports configured in CNA or NIC mode)
- DCB status and statistics (CNAs and Fabric Adapter ports configured in CNA mode only)
- Network driver information, Ethernet statistics, offload parameters, and flow control coalesce parameters (CNAs and Fabric Adapter ports configured in CNA or NIC mode only)
- Ethernet offload, flow control, and coalescing parameters (CNAs and Fabric Adapter ports configured in CNA or NIC mode only)

NOTE
Before collecting data through the Support Save feature, you may want to disable auto-recovery on the host system. This is because when adapters are reset after an auto-recovery from a failure, traces initiated before the failure may be lost or overwritten.

To disable auto-recovery, use the following commands.

- For Linux, use the following commands.
  - To disable auto-recovery for the network (BNA) driver.

    ```
    insmod bna.ko bnad_ioc_auto_recover=0
    ```

  - To disable auto-recovery for the storage (BFA) driver.

    ```
    insmod bfa.ko bnad_ioc_auto_recover=0
    ```

- For VMware, use the following commands.
  - To unload and load the network (BNA) driver with IOC auto-recovery disabled, use the following commands.

    ```
    esxcfg-module -u bna
    esxcfg-module bna bnad_ioc_auto_recover=0
    ```

  - To disable IOC auto-recovery for the BNA driver across reboots, use the following command.

    ```
    esxcfg-module -s "bnad_ioc_auto_recover=0" bna
    ```

  - To unload and load the network (BFA) driver with IOC auto-recovery disabled, use the following commands.

    ```
    esxcfg-module -u bfa
    esxcfg-module bfa bfad_ioc_auto_recover=0
    ```

  - To disable IOC auto-recovery for the BFA driver across reboots, use the following command.

    ```
    esxcfg-module -s "ioc_auto_recover=0" bfa
    ```

- For Windows, use the Registry Edit tool (regedt32) or the BCU **drvconf –key** command. Following is the **drvconf —key** command.

```
bcu drvconf --key ioc_auto_recover --val 0
```

- For Solaris, edit /kernel/drv/bfa.conf using the following.

```
ioc_auto_recover=0
```

NOTE
Brocade 804 and 1007 adapters are not supported on Solaris systems so Solaris commands do not apply to these adapters.

Initiating Support Save through HCM

Launching the Support Save feature in HCM collects HCM application data. Initiate Support Save by selecting **Tool > Support Save**.

Messages display during the Support Save operation that provide the location of the directory where data is saved. If you are initiating Support Save from a remote management station and receive a warning message that support files and Agent logs could not be collected, the HCM Agent is unavailable on the remote host. Select **Tool** > **Backup** to backup data and configuration files manually.

Support data is collected to a file in your system's tmp directory by default.

For more information and additional options for using this feature, refer to the *Brocade Adapters Administrator's Guide*.

Initiating Support Save through Management applications

To capture technical support and event information for installed adapters in Management applications, such as Network Advisor, complete the following steps.

1. Select **Monitor > Technical Support > SupportSave**.

   The **Technical SupportSave** dialog box displays.

2. Click the **Generate Now** tab.
3. Click the **Hosts** tab.
4. Right-click in the **Available Hosts** table and select **Expand All**.
5. Select the host where adapters are installed, and click the right arrow to move them to the **Selected Switches and Hosts** table.

5. Click **OK** on the **Technical SupportSave** dialog box.

6. Click **OK** on the confirmation message.

To view Support Save information use the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Repository** dialog box displays.

2. Select the **Hosts** tab to view technical support information on hosts.

3. Click **View** to view the repository in an Internet browser window.

   The technical support information displays in an Internet browser window.

Initiating Support Save through BCU commands

Launching the Support Save feature using the **bfa_supportsave** command collects information for the selected adapter. For information on entering BCU commands, refer to "Using BCU commands" on page 65.

The **bfa_supportsave** command creates and saves the supportsave data to the following locations:

- The /tmp directory on Linux and Solaris systems.
- The current directory for Windows systems.

Following are examples of other parameters you can use with this command:

- bfa_supportsave <dir> - Creates and saves the supportsave data under a directory name that you provide.
- bfa_supportsave <dir> <ss_file_name> - Creates and saves the supportsave data under a directory and file name that you provide. If the directory already exists, it will be overwritten.

NOTE
If specifying a directory, make sure that the directory does not already exist to prevent overwriting the directory. Do not just specify a driver (such as C:) or C:\Program Files.

Messages display as the system gathers information. When complete, an output file and directory display. The directory name specifies the date when the file was saved.

For more information and additional options for using this feature, refer to the *Brocade Adapters Administrator's Guide*.

Using supportsave on VMware ESX systems

For VMware ESX 5.0 and later systems, BCU commands are integrated with the esxcli infrastructure. Enter the following to initiate the BCU supportsave command:

```
esxcli brocade supportsave
```

Initiating Support Save through the internet browser

Launching Support Save through the internet browser collects information for adapters installed on a selected host system. Use the following steps to launch this feature.

1. Open an Internet browser and type the following URL.

   ```
   https://localhost:34568/JSONRPCServiceApp/SupportSaveController.do
   ```

   where localhost is the IP address of the host system from which you want to collect the **bfa_supportsave** information.

2. Log in using the factory default user name (admin) and password (password). Use the current user name and password if they have changed from the default.

   The **File Download** dialog box displays, prompting you to save the `supportSaveController.do` file.

3. Click **Save** and navigate to the location where you want to save the Support Save file.

4. Save the file, but rename with a “zip” extension. For example,

   `supportSaveController.zip.`

5. Open the file and extract contents using any compression utility program.

Initiating Support Save through a port crash event

If the port crashes and triggers a port crash event, Support Save data is collected at a system-wide level. An Application Log message is generated with the following message.

```
Port Crash Support Save Completed
```

Port crash events have a CRITICAL severity and you can view the details in the Master Log and Application Log tables in HCM. For more information on these logs, refer to “HCM logs” on page 70.

Support Save differences

Following are differences in data collection for the HCM, BCU, and browser applications of **bfa_supportsave**:

- BCU - Collects driver-related logs, HCM Agent information, and configuration files.
- Browser - Collects driver-related and HCM Agent logs and configuration files.
- HCM - Collects HCM application data, driver information, HCM Agent logs, and configuration files.

NOTE
HCM Master logs and application logs are saved when Support Save is initiated through HCM, but not through the BCU command.

Using BCU commands

To use BCU commands, enter commands at the BCU> command prompt. For Windows systems, open the command prompt using the Brocade BCU desktop shortcut, which is automatically installs to your desktop with the adapter software. Note that if installation fails (for example, because devices are not present on the system), the shortcut is still created. The BCU shortcut provides quick access to the installation folder where you can perform the following tasks:

- Run the Support Save feature
- Reinstall drivers
- Run adapter utilities

NOTE
Launching BCU on Windows systems through methods other than through the desktop shortcut is not recommended and may result in display of inconsistent information.

To list all the commands and subcommands, type the following command:

bcu –help

To check the CLI and Driver version number, type the following command:

bcu –version

For complete details on BCU commands, refer to the *Brocade Adapters Administrator’s Guide*.

VMware ESX 5.0 and later systems

For VMware ESX 5.0 and later systems, BCU commands are integrated with the esxcli infrastructure.

To run a BCU command, use the following syntax:

```
esxcli  brocade bcu --command=" command"
```

where:

command BCU command, such as **port –list**.

For example:

```
esxcli  brocade bcu --command="port -list"
```

Data collection using Fabric OS commands (Brocade switches only)

Use the following Fabric OS commands on attached Brocade switches to gather information and help isolate connectivity and other problems between the adapter, switch, and storage ports. For details on using these commands, refer to the *Fabric OS Command Reference Manual*.

- **authUtil**

  Use this command to display and set local switch authentication parameters.

- **cfgShow**

  Use this command to display zone configuration information for the switch. You can use command output to verify target ports (by port WWN) and LUNs that are intended to be accessible from the adapter.

- **fcpProbeShow**

  Use this command to display the Fibre Channel Protocol daemon (FCPd) device-probing information for the devices attached to a specified F_Port or FL_Port. This information includes the number of successful logins and SCSI INQUIRY commands sent over this port and a list of the attached devices.

- **nsShow**

  Use this command to display local NS information about all devices connected to a specific switch. This includes information such as the device PID, device type, and the port and node WWN.

- **zoneshow**

  Use this command without parameters to display all zone configuration information (both defined and enabled).

- **portErrShow**

  Use this command to display an error summary for all switch ports.

- **portLogShow**

  Use this command to display the port log for ports on a switch.

- portLogShowPort

  Use this command to display the port log for a specified switch port.

- portPerfShow

  Use this command to display throughput information for all ports on the switch.

- portStatsShow

  Use this command to display hardware statistics counters for a specific switch port.

- portShow

  Use this command to display information and status of a specified switch port, including the speed, ID, operating state, type, and WWN.

- SecAuthSecret

  Use this command to manage the DH-CHAP shared secret key database used for authentication. This command displays, sets, and removes shared secret key information from the databases.

- sfpShow

  Use this command to display detailed information about specific SFPs installed in a switch. This command is supported on stand-up adapters only.

- show vlan brief

  Displays information about a VLAN interface on the switch.

- show dcb maps

  Displays information about the configured DCB maps in the switch.

- switchShow

  Use this command to display switch and port information. Output may vary depending on the switch model. Use this information to determine the fabric port WWN and PID connected to an adapter port. Also display topology, speed, and state of each port on the switch.

- trunkshow

  Use this command to display trunking information for the switch, such as the configuration, bandwidth, and throughput of trunk groups.

Adapter event messages

When applicable events occur during adapter operation, the adapter driver generates event messages. These messages are captured in your host system logs. These messages are also captured in an agtEvent.log file by the HCM and displayed in the HCM master log. Note that message display may differ in your host system log and the HCM master log, however messages may contain the following information:

- Message ID
- Description
- Severity level
- Event category
- Cause of event
- Recommended action

- Date and time event occurred

NOTE
For details of all driver event messages, refer to Appendix A, "Adapter BIOS and Event Message Reference".

Message details are also contained in HTML files, which load your system when you install the adapter driver. You can view these HTML files using any internet browser application. Table 6 provides the default location where these message files install for each supported operating system.

TABLE 6 Message catalog location

Operating System	Catalog Location
Linux	/opt/bfa
VMware	/opt/bfa
Solaris	/opt/bfa
Windows	aen.zip loaded to your driver installation directory. Unzip this file to obtain all message catalog files.

Table 7 lists the message file names and content for the message files.

TABLE 7 Event message files

Event Catalog File	Content
bfa_aen_adapter.html	Adapter events, such as adapter added or removed
bfa_aen_audit.html	Audit events, such as authentication enabled or disabled for base port
bfa_ethport.html	Base port Ethernet events, such as the Ethernet link up and link down.
bfa_aen_ioc.html	I/O controller (IOC) events.
bfa_aen_itnim.html	Initiator-target nexus events.
bfa_aen_lport.html	Logical port events.
bfa_aen_port.html	Physical base port events.
bfa_aen_rport.html	Remote port (R_Port) events.
hba_error_codes.doc	List of error codes and meanings for the following events: • Adapter - events relating to the adapter • Physical port • L_Port - logical port • R_Port - remote initiator or target port • ITNIM - initiator target nexus • Audits • IOC - I/O controller • Ethernet port

NOTE
Complete content for adapter driver event messages is included in Appendix A, "Adapter BIOS and Event Message Reference".

Logs

Event and error messages that occur during adapter, driver, and HCM operation are important tools for isolating and resolving problems. These messages provide descriptions of an event or problem, severity, time and date of the event, and in some cases, cause and recommended actions. Messages are captured in logs available through HCM, BCU commands, and through host system commands. Monitoring events and errors in these logs allows early fault detection and isolation on a specific adapter.

Host system logs

Brocade adapter event messages are captured in host system log files. All messages related to the Brocade adapter are identified in these logs by BFA (Brocade fabric adapter), BNA (Brocade network adapter), and BFAL (Brocade fabric adapter library]. Table 8 describes the logs for each supported operating system where adapter event messages display and how to view these logs.

TABLE 8 System event Logs

Operating System	Log Name	Location	Viewing Message Log
Solaris[1]	Syslog	/var/adm/messages	dmesg command
Windows	Event Log	Not applicable	• System category in Event Viewer (eventvwr.exe) • bcu winlog command[2]
Linux	Messages Log	/var/log/message	dmesg command
VMware[3]	Messages Log	/var/log/message* , /var/log/vmkernel*, /var/log/vmkwarning*, /proc/vmware/log	dmesg command

1. Brocade 804 and 1007 adapters are not supported on Solaris systems.
2. Supported on Windows systems only.
3. For ESX Server platforms. For Guest system, refer to information in Windows or Linux.

Syslog support

You can configure the HCM Agent to forward events to a maximum of three system log destinations using the **Syslog** option on the HCM **Configure** menu. These events will display in the operating system logs for systems such as Solaris and Linux. For procedures to configure syslog destinations, refer to the *Brocade Adapters Administrator's Guide*.

HCM logs

You can view data about adapter operation through HCM logs that display in HCM. These logs display on the bottom of the HCM main window. Click the **Master Log** or **Application Log** to toggle between the following logs:

- The **Master Log** displays informational and error messages during adapter operation. This log contains the severity level, event description, date and time of event, and the function that reported the event (such as a specific adapter port or remote target port).
- The **Application Log** displays informational and error messages related to user action in HCM, discovery, or HCM application issues.

Master Log

The **Master Log** displays event information in seven fields:

- Sr No.

  Sequence number assigned to the event when it occurred, in ascending order.

- Severity

  Event severity level (informational, minor, major, or critical).

  - Critical-level messages indicate that the software has detected serious problems that will eventually cause a partial or complete failure of a subsystem if not corrected immediately. For example, IO controller heartbeat failure is a critical error.
  - Major messages represent conditions that do not impact overall system functionality significantly.
  - Minor messages highlight a current operating condition that should be checked or it might lead to a failure.
  - Information-level messages report the current non-error status of the system components, for example, the online and offline status of a port.

- WWN

  World-Wide Name of adapter where the event occurred.

- Category

  The category or type of event. Categories define the component where events occur:

  - ADAPTER - Events pertaining to the adapter.
  - PORT - Events pertaining to a physical port.
  - LPORT - Events pertaining to a specific logical port (one logical port always exists per physical port).
  - RPORT - Events pertaining to a specific remote port (could be an initiator or target).
  - ETHPORT - Events pertaining to the Ethernet port.
  - AUDIT - Audit events subcategory.
  - IOC - Events pertaining to the I/O controller.
  - ITNIM - Events pertaining to an initiator-target nexus.
  - VLAN - Events pertaining to a virtual LAN.
  - TEAM - Events pertaining to a team (link aggregation group).

- Subcategory of main category.

- Event description, Date, and Time

  Brief description of event and date and the time when the event occurred.

NOTE
Complete content of adapter event messages is provided in Appendix A, "Adapter BIOS and Event Message Reference".

You can block events from displaying in the **Master Log** by severity, category, and WWN of adapter using the **Master Log Filter** dialog box. To display this dialog box, click the **Filter** button in the **Master Log** section of the main HCM screen. Select areas that you want to filter and click **OK**.

Application Log

The **Application Log** displays all application-related informational and error messages, as well as the following attributes:

- Date and time the message occurred.
- Severity of the message.
- Description of the message.
- The Agent IP address.

Logging levels adjustment

Adjust the logging level for related adapter logs using BCU commands and HCM options. By adjusting the logging level, you can control the number and type of messages that are captured the log.

NOTE
For greater detail on adjusting logging levels, refer to the *Brocade Adapters Administrator's Guide*.

Adjusting the adapter event logging level

Specify the number of event messages logged by the host system log for the storage driver using this BCU command.

Port logging level

Adjust logging level for port logs using BCU commands and HCM.

Adjusting the port logging levels through HCM

Use the following steps to adjust port logging level for CNAs, HBAs, and Fabric Adapter ports configured in CNA or HBA mode.

1. Select a host, adapter, or adapter port from the device tree.
2. Select **Configure** > **Basic Port Configuration** from HCM.

   The **Basic Port Configuration** dialog box displays.
3. Select a value from the **Port Logging Level** list.

   Supported values are Log Critical, Log Error, Log Warning, and Log Info.

Click **Apply** to apply the changes.

4. Click **OK** to save the changes and close the window.

Use the following steps to adjust port logging level for Fabric Adapter ports configured in NIC mode.

1. Select an Ethernet port from the device tree.
2. Select **Configure** > **Eth Configuration**.

   The **Eth Configuration** dialog box displays.
3. Select a value from the **Port Logging Level** list.

   Supported values are Log Critical, Log Error, Log Warning, and Log Info.
4. Click **OK** to save the changes and close the window.

Adjusting the port logging level through BCU

```
bcu log --level <port_id> [<level>]
```

where:

port_id	The ID of the port for which you want to set the log level. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.
level	Critical | Error | Warning | Info Specifies the severity level. Error is the default setting. If no level is specified, the current log level displays.

Configure logging levels for HCM logs

Adjust the number of messages logged to the following HCM logs:

- Agent Communication Log, where all messages are exchanged between the HCM application and the HCM Agent.
- HCM Debug Log, where messages are logged locally.

To adjust the logging level, use the following steps.

1. Select **Configure** > **HCM Logging Levels** to display the HCM Logging Levels dialog box.
2. Select a level on the **Agent Communication Log** and **HCM Debug Log** lists.

   Values are Trace, Debug, Info, Warning, Error, and Fatal.

Statistics

You can access a variety of statistics using BCU commands and HCM. Use these statistics to monitor adapter performance and traffic between the adapter and LUNs and isolate areas that impact performance and device login.

You can display statistics for the following:

- Adapter ports
- Authentication activities
- DCB
- Fibre Channel over Ethernet (FCoE)
- Firmware
- vHBA
- vNIC
- Virtual ports (vport)
- Link Layer Discovery Protocol (LLDP)
- Logical ports (lport)
- Remote ports (rport)
- Fibre Channel Protocol (FCP) initiator mode
- Fabric
- Teaming
- Targets
- Teaming
- Trunking
- Real-time performance of DCB port
- Security authentication
- VLAN
- vHBA

This section provides an overview of these statistics and how to access them. For more detail, refer to the *Brocade Adapter's Adapters Administrator's Guide*.

Authentication statistics

Use BCU commands and HCM to display statistics related to transmitted and received DH-CHAP attempts for a selected port. You can display statistics such as the following:

- The number of times security authentication failed
- The number of times security authentication succeeded
- The number of rejected transmitted Fibre Channel authentication attempts (Tx Auth Rjts)
- The number of transmitted Fibre Channel authentication negotiation attempts (Tx Auth Negs)
- The number of completed Fibre Channel authentication negotiation attempts (Tx Auth Dones)
- The number of transmitted DH-CHAP replies (Tx DHCHAP)
- The number of transmitted DH-CHAP challenge attempts (Tx DHCHAP Challenges)

- The number of times a transmitted Fibre Channel authentication attempt was successful (Tx DHCHAP Successes)
- The number of rejected received Fibre Channel authentication attempts (Rx Auth Rjts)
- The number of received Fibre Channel authentication negotiation attempts (Rx Auth Negs)
- The number of completed received Fibre Channel authentication attempts (Rx Auth Dones)
- The number of received DH-CHAP challenge attempts (Rx DHCHAP Challenges)
- The number of received DH-CHAP replies (Rx DHCHAP Replies)
- The number of times a received DH-CHAP challenge was successful (Rx DHCHAP Successes)

Displaying statistics through BCU

Use the following BCU command to display authentication statistics for CNAs and Fabric Adapter ports configured in CNA mode.

```
bcu auth --stats <port_id>
```

where:

<port_ID> The ID of the Ethernet port. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

Displaying statistics through HCM

Display the **Authentication Statistics** dialog box using the following steps.

1. Select an HBA port or Fabric Adapter port configured in HBA mode from the device tree.
2. Select **Configure > FC_SP > Authentication Statistics**.

DCB statistics (CNA only)

Use BCU commands and HCM to display Data Center Bridging (DCB) statistics for CNAs or Fabric Adapter ports configured in CNA mode. Statistics such as the following display:

- Logical link layer discovery protocol (LLDP) frames transmitted, received, timed out, discarded, with error, type-length-values (TLVs) discarded, and TLVs unrecognized.
- Data center bridging capability exchange (DCBX) TLVs unrecognized, negotiation fails, remote configurations changed, TLVs received and invalid, status up and down, and received invalid configurations.

Displaying statistics through BCU

Use the following BCU command to display DCB statistics.

```
bcu dcb --stats <port_id>
```

where:

<port_ID> The ID of the Ethernet port. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

Displaying statistics through HCM

Display the **DCB Statistics** dialog box using the following steps.

1. From the device tree, select a physical port of a CNA or Fabric Adapter ports configured in CNA mode.
2. Select **Monitor > Statistics > DCB Statistics**.

DCB query (CNA only)

Use this query for CNAs or to Fabric Adapter ports configured in CNA mode only. Query the DCB information on a selected port and display such information as LLDP attributes and the DCB group map priority tables.

```
bcu dcb --query <port_id>
```

where:

<port_ID> The ID of the Ethernet port. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

FCoE statistics (CNA)

These statistics are available on CNAs and on Fabric Adapters configured in CNA mode. Use BCU and HCM to display statistical information related to a selected Fibre Channel over Ethernet (FCoE) port. Statistics include the number of transmitted and received packets and transmitted and received bytes. You can also select options to continue running data, configure polling frequency, and start polling.

Displaying FCoE statistics through BCU

Use the **fcoe –stats** command to display FCoE statistics.

```
fcoe --stats <port_id>
```

where:

port_id — ID of the adapter port for which you want to display statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

Displaying FCoE statistics through HCM

To display FCoE statistics through HCM, use the following steps.

1. Select an FCoE port from the device tree.
2. Select **Monitor** > **Statistics** > **FCoE Statistics** from the device tree.

   OR

   Right-click the FCoE port and select **Statistics** > **FCoE Statistics** from the list.

   The **FCoE Statistics** dialog box at the host level displays.

Fabric statistics

Use BCU and HCM to display statistics for fabric login (FLOGI) activity and fabric offlines and onlines detected by the port. Use these statistics to help isolate fabric login problems. Examples include number of FLOGIs sent, FLOGI response errors, FLOGI accept errors, FLOGI accepts received, FLOGI rejects received, unknown responses for FLOGI, allocation waits prior to sending, the number of delayed fabric login allocations, FLOGIs received, and incoming FLOGIs rejected.

Following are two examples of how to use these statistics for troubleshooting:

- If the adapter is not showing in the fabric, check the FLOGI sent and FLOGI accept statistics. If the counts do not match, the switch or fabric may not be ready to respond. This is normal as long as it does not persist. If the problem persists, this could indicate a problem in the fabric or a protocol issue between the adapter and fabric.
- If fabric offline counts increase and fabric maintenance is not being done, this may indicate a serious fabric problem. Slow fabric performance or hosts unable to address storage could also be seen.

Displaying fabric statistics through BCU

Use the **fabric –stats** command to display fabric statistics.

```
fabric --stats <port_id>
```

where:

port_id — ID of the adapter port for which you want to display statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

Displaying fabric statistics through HCM

Use the **Fabric Statistics** dialog box to monitor a variety of port data.

1. Launch the HCM.
2. Select the FC port from the device tree window.
3. Click **Monitor > Statistics > Fabric Statistics**.

Displaying FCP initiator mode statistics

Use the **fcpim –stats** command to display FCP initiator mode statistics and attributes.

```
fcpim --stats <port_id> <pcifn> <rpwwn> [-l <lpwwn>
```

where:

stats	Displays FCP initiator mode statistics.
pcifn	PCI function number associated with the physical port.
-l lpwwn	Logical PWWN. This is an optional argument. If the -l lpwwn argument is not specified, the base port is used.
-l rpwwn	Remote PWWN.

To clear FCP initiator mode statistics, enter the following command.

```
fcpim --statsclr <pcifn> <rpwwn [-l <lpwwn>]
```

FCP initiator mode statistics

Use HCM to display FCP IM module statistics for each initiator target nexus (ITN). Statistics display such as I/Os waiting for circular queue space, number of I/O context requests, I/O abort requests, number of task management I/O context requests, I/O completions with OK status, number of successful firmware I/O underrun operations, number of successful firmware I/O overrun operations, aborted I/O requests, I/O timeouts, I/O selection timeouts, I/O protocol errors, host I/O abort requests, PRLI statistics, and remote port statistics.

Use the following steps to display the **FCP IM Statistics** dialog box.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > FCP IM Module Statistics**.

   or

   Right-click a port from the device tree and select **Statistics** > **FCP IM Module Statistics.**

Enabling and disabling profiling for FCP initiator mode statistics through BCU

When profiling is enabled, I/O latency data is distributed based on I/O size (average, minimum, and maximum). You can use this to study typical application I/O patterns, and this may help in tuning adapters, fabric, and targets for better performance. You must run the **fcpim –stats** command to display this data.

NOTE
Enabling profiling will impact I/O performance, so use this command to analyze traffic patterns and not in production systems.

Use the following command to enable profiling.

```
fcpim --profile_on <port_id>
```

Use the following command to disable profiling.

```
fcpim --profile_off <port_id>
```

where:

port_id	ID of the port for which you want to enable or disable profiling. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

Firmware statistics

Use HCM to display I/O controller (IOC) firmware statistics for the following categories:

- IOC firmware
- IOC Fibre Channel (FC) firmware
- Firmware IO (Initiator Mode)
- Firmware port FPG

Use the following steps to display the **Firmware Statistics** dialog box.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > Firmware Statistics**

   or

   Right-click a port from the device tree and select **Statistics** > **Firmware Statistics.**

I/O performance

Use the **fcpim -ioperf** command to display I/O performance in terms of IOPs and throughput for physical ports and I-T nexus (ITN) sessions for a logical port. Use the command with a physical port range or with a specific physical port ID.

Using port range

The following command displays IOPs and throughput for a range of physical ports.

```
--ioperf <port_range> [-l | -r] [-c count] [-i interval]
```

where:

port_range	This is the adapter number/port number-adapter number/port number. For example, the range 1/0-2/0, includes adapter 1, port 0 and adapter 2, port 0.
-l	Displays information about all logical ports in all physical ports in the range.
-r	Displays information about all ITM sessions in all physical ports in the range. This includes all logical and remote port information.
-c	Count. The number of iterations of the display. The default behavior is to continuously refresh. Use Ctrl-C to terminate.
-i	Interval. The sampling delay in seconds [default is 1 second]. The sampling interval can be between 1 and 10.

Using specific port ID

The following command displays IOPs and throughput for a specific physical port ID.

```
--ioperf <port_ID> <port_id> [-l <lpwwn>] [-r <rpwwn>] [-c count] [-i interval]
```

where:

port_id	ID of the port for which you want to display statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.
-l pwwn	Displays information about a specific logical port for the physical port. To display data about all logical ports, use -l without a PWWN.
-r pwwn	Displays information at I-T nexus between a given logical port and specified remote port for the physical port. To display data about all remote ports, use -r without a PWWN.
-c	Count. The number of iterations of the display. The default behavior is to continuously refresh. Use Ctrl-C to terminate.
-i	Interval. The sampling delay in seconds [default is 1 second]. The sampling interval can be between 1 and 10.

Logical port statistics

Use HCM and BCU to display logical port statistics for the following:

- Discover address (ADISC)
- Name server (NS) port logins (plogin) activity
- NS port response activity
- NS command activity
- Register symbolic port name (RSPN_ID) identifier activity
- Register FC4 type identifier (RFT_ID) activity
- Register FC4 type identifier (RFT_ID) activity
- “Get all port ID requests” for a given FC4 type (NS_GID_FT) activity
- Port logout (LOGO)
- MS command activity
- MS port login activity
- Port login (PLOGI)
- Process login (PRLI)
- Process logout (PRLO)
- Retries
- Timeouts
- Registered state change notifications (RSCN) received
- Received ELS command activity
- Virtual port performance

Use these statistics to help determine if the adapter is not registering with the name server or cannot access storage. Following are examples of how these statistics indicate these problems:

- If name server port login (NS PLOGI) error rejects and unknown name server port login response (NS login unknown rsp) errors increase, then the adapter most likely cannot log in to the name server.
- If name server register symbolic port name identifier (NS RSPN_ID) or name server register symbolic port name identifier response (NS RFT_ID rsp) errors or rejects (NS RFT_ID rejects) are increasing, the adapter has a problem registering with the name server.
- If name server “get all port ID response” NS GID_FT rsp), rejects (NS_GID FT rejects), or unknown responses (NS_GID FT unknown rsp) are increasing, the adapter has a problem querying the name server for available storage.

Displaying logical port statistics through HCM

Display logical port statistics by selecting **Monitor > Statistics > Logical Port Statistics.**

OR

Right-click a logical port from the device tree and select **Logical Port Statistics**.

Displaying logical port statistics through BCU

Use the **lport –stats** command to display logical port statistics.

```
lport --stats <port_id> [-l <lpwwn>]
```

where:

port_id	ID of the port for which you want to display statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.
-l lpwwn	Logical port world wide name for which you want to display statistics. This is an optional argument. If the -l lpwwn argument is not specified, the base port is used.

Performance data

Using HCM, you can collect real-time and historical performance data on the following managed devices:

- Port statistics for the adapter.
- Virtual Port statistics on the virtual port
- Ethernet statistics on the Ethernet node
- FCP IM statistics on the remote port

Data is displayed in graphs using utilization (Mbps) and errors per second. Polling intervals can be configured to 10, 20, and 30 seconds. Data collected will not be lost once the graph is closed.

To generate a real-time performance graph for a device, complete the following steps.

1. Select the device (such as adapter, remote port, virtual port) Ethernet node) for which you want to generate a real-time performance graph.
2. Select **Configure > Performance > Realtime Statistics**.

PHY module statistics

The Ethernet PHY module, located in the mezzanine card port hardware, aids in communications to and from the Ethernet LAN. Use the **bcu phy –stats** command to display the following statistics:

- PHY status
- Line breaks after linkup
- PMA (physical medium attachment sublayer) and PMD (physical medium dependent sublayer) receive and transmit faults
- PCS (physical coding sublayer) receive and transmit faults
- Speed negotiations
- Transmit EQ trainings and timeouts
- CRC errors

```
bcu phy --stats <port_id>
```

where:

<port_id>	ID of port for which you want to display statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

Port Performance

Use the BCU port --perf command to display throughput information, in number of bytes received and transmitted, for a specific physical port.

```
port --perf <port_range|all> [-c count] [-i interval]
```

where:

port_range	Port range to be displayed. If the range exceeds 80 columns, a warning displays. The maximum ports within the 80 column limit will display. Specify port range as the adapter number/port number-adapter number/port number. For example, the range 1/0-2/0, includes adapter 1, port 0 and adapter 2, port 0.
c	Count. The number of iterations of the display. The default behavior is to continuously refresh. Use Ctrl-C to terminate.
-i	Interval. The sampling delay in seconds [default is 1 second]. The sampling interval can be between 1 and 10.

ESX 5.0 systems

On ESX 5.0 and later systems, the port --perf will not work unless the -c option is used. The -c option can be any number (limited by esxcli buffer size). For example, you can use the following:

```
esxcli brocade bcu --command="port --perf -c 1"
```

For more information on using BCU commands on ESX 5.0 and later systems, refer to "VMware ESX 5.0 and later systems" on page 66

Port statistics

Use BCU and HCM to display a variety of port statistics. Following is an overview of port statistics for different adapter types:

- For HBAs and Fabric Adapter ports configured in HBA mode, statistics include transmitted and received frames and words, received loop initialization primitive (LIP) event counts, error frames received, loss of synchronization, link failure and invalid CRS counts, end of frame (EOF) errors, encoding non-frame errors, and credit recovery statistics. Use these statistics to isolate link and frame errors. For example, loss of synch and loss of signal errors indicate a physical link problem. To resolve these problems, check cables, SFPs on adapters (stand-up adapters only) or switch, and patch panel connections.
- For CNAs and Fabric Adapter ports configured in CNA mode, statistics include total transmit and receive counts for different sizes and types of frames. Data is included on 64-byte to 1519-1522-byte, multicast, broadcast, control, jabber, drop, control, FCS error, alignment error, code error, pause MAC control, zero pause MAC control, FCoE pause MAC control, and zero pause MAC control frames.

Displaying statistics through BCU

Use the **port –stats** BCU command to display statistics for a specified adapter port.

```
port --stats <port_id>
```

where:

port_id	ID of the port for which you want to display statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

Displaying statistics through HCM

Use the **Port Statistics** dialog box to monitor a variety of port data. Launch this dialog box using the following steps:

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > Port Statistics**.

Real-time and historical performance statistics

Use HCM to collect and display real-time and historical performance data in graphs for the following counters.

- Tx bytes (Mbps)
- Rx bytes (Mbps)
- Tx drops
- Rx drops—The number of dropped received frames
- Tx FCS errors
- Rx FCS errors
- Rx packets

Display statistics for the following managed devices:

- Ports on all adapter types.
- Virtual ports
- Ethernet ports on the Ethernet node (CNAs and Fabric Adapter ports configured in CNA or NIC mode)
- Remote port (FCP IM statistics)

You can launch graphs for multiple ports to observe the historical trend or real-time behavior of statistics across multiple ports. You can also change the polling intervals in seconds for collecting data to display.

To generate a real-time performance graph for a device, use the following steps.

1. Select a device port in the device tree.
2. Select **Configure > Performance > Realtime Statistics** to display the **Realtime Performance** dialog box.

3. Select the type of statistics that you want to run from the Statistics Name list.
4. Select the polling interval.
5. Click **Apply** to save your changes.

To display the **Historical Performance** dialog box and graphs for a port, use the following steps.

1. Select a device for which you want to generate a historical performance graph.
2. Select **Monitor > Performance.**
3. Select the **Enable Historical Data Collectio**n check box to display the Historical Performance dialog box.
4. Select the type of statistics that you want to run from the **Statistics Name** list.
5. Click **Apply** to save your changes.

Remote port statistics

Remote port statistics can help isolate end-to-end login problems. Use HCM and BCU to display statistics for the following:

- Port login (PLOGI) activity
- Authentication and discovery (ADISC) activity
- Logout (LOGO) activity
- RCSNs received
- Process logins (PRLI) received
- Hardware abstraction layer (HAL) activity
- Remote port speed capability (RPSC)

As an example of using these statistics for troubleshooting, if the host cannot see the target, you can verify that the remote port (rport) is reporting itself online by comparing the rport offline and rport online statistics. The rport online counter should be one greater than the rport offline counter. If not, clear the counters and retry connecting to the remote port. Verify the rport online and rport offline statistics again.

Displaying target statistics through HCM

Launch the **Target Statistics** dialog box using the following steps to display target statistics.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > Remote Port Statistics > Target Statistics**.

Displaying remote port statistics through BCU

Use the **rport –stats** command to display remote port statistics.

```
rport --stats <port_id> <rpwwn> [-l <lpwwn>]
```

where:

port_id	ID of the port for which you want to display rport statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.
lpwwn	Displays the logical PWWN. This is an optional argument. If the -l lpwwn argument is not specified, the base port is used.
rpwwn	Displays the remote port's PWWN.

Quality of Service statistics (HBA)

Use HCM and BCU to display quality of service (QoS) statistics for individual HBA ports and Fabric Adapter ports configured in HBA mode. You can display statistics for fabric login (FLOGI) activity, exchange link parameter (ELP) activity, and received QOS registered state change notifications (RSCNs).

Displaying QoS statistics through HCM

Use the **QOS Statistics** dialog box to display QoS statistics.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Remote Port Statistics > QOS Statistics**.

Displaying QoS statistics through BCU

Use the **qos –stats** command to display remote port statistics.

```
qos --stats <port_id> <vpwwn>
```

where:

port_id	ID of the port for which you want to display QoS statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

Trunking attributes

Use the bcu **trunk –query** command to display trunk attributes for the adapter.

```
trunk --query <ad_id>
```

where:

ad_id	ID of the adapter.

vHBA statistics

Display vHBA statistics on HBAs, CNAs, or Fabric Adapter ports configured in HBA or CNA mode. Use HCM and BCU to display statistics related to virtual host bus adapters (vHBA) associated with an FC or FCoE port. Statistics such as the following display:

- Polling frequency
- Heartbeat failures
- Firmware boots
- vHBA statistics timeouts
- Enable/disable replies
- Enable/disable requests
- I/O path TOVs expired
- I/O clean-up requests
- IT Nexus onlines, offlines, create requests
- TM requests
- I/O timeouts
- Total I/O count
- TM cleanup requests, completions
- Host abort requests

Displaying statistics through HCM

To display statistics, perform the following steps:

1. Launch the HCM.
2. Select an FC or FCoE port from the device tree
3. Click **Monitor > Statistics > vHBA Statistics**.

The **vHBA Statistics for FCoE Port** dialog box displays.

Displaying statistics through BCU

Use the **vhba –stats** command to display remote port statistics.

```
vhba --stats <pcifn>
```

where:

pcifn PCI function number associated with the vHBA.

vNIC statistics (CNA or NIC)

Display virtual Network Interface Card (vNIC) statistics on Fabric Adapter ports configured in CNA or NIC mode. Use HCM and BCU to display statistics, which are relevant to the Ethernet I/O controller (IOC). Statistics such as the following display:

- Mailbox interrupts
- Enable and disable events

- Heartbeat failures
- Firmware boots
- vNIC statistics timeouts
- Disable and enable requests
- Disable and enable replies
- Link toggle count
- CEE toggle count
- BPC statistics
- RAD statistics
- Ethernet ICO statistic timeouts

You can also select options to keep running data, set the polling frequency, start polling data, and reset statistics.

Displaying statistics through HCM

To display statistics, perform the following steps:

1. Launch the HCM.
2. Select an FC or FCoE port from the device tree
3. Click **Monitor > Statistics > vNIC Statistics**.

The **vNIC Statistics for Eth Port** dialog box displays.

Displaying statistics through BCU

Use the **vnic–stats** command to display remote port statistics.

```
vnic --stats <pcifn>
```

where:

pcifn PCI function number associated with the vNIC.

Virtual port statistics

Use HCM and BCU to display logical port statistics for fabric discovery (FDISC) activity, logouts (LOGO) activity, NPIV support, number of fabrics online and offline, and fabric cleanups.

Use these statistics to isolate NPIV login problems. Following are examples of what to check if virtual devices are not listed in the name server:

- If FDISC sent and FDISC accept statistics do not match, the fabric or switch may not be ready for data transmission. This is normal as long as it does not persist. If it does persist, there may be a problem in the fabric or a protocol issue between the adapter and fabric. Note that in this case FDISC retries also increase.
- Check the No NPIV support statistics to verify that NPIV is supported and enabled on the switch.

Displaying virtual port statistics through HCM

Display statistics by selecting **Monitor > Statistics > Virtual Port Statistics.**

OR

Right-click a virtual port on the device tree and select **Virtual Port Statistics**.

Displaying virtual port statistics through BCU

Use the **vport –stats** command to display statistics.

```
vport --stats <port_id> <vpwwn>
```

where:

port_id	ID of the port for which you want to display virtual rport statistics. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.
vpwwn	Displays the statistics for the virtual port by its WWN. If no PWWN is specified, the information provided is for the base vport.

VLAN statistics for a team (CNA and NIC)

Use HCM and BCU to display VLAN statistics for a team that use CNA ports or Fabric Adapter ports configured in CNA or NIC mode. VLAN statistics related to a specific team can include VLAN ID, VLAN name, number of transmit and receive bytes, length of time between byte transmission and reception, and correction status. You can also use options to set the polling frequency, start polling, and reset statistics.

Displaying VLAN statistics through HCM

VLAN statistics for a team can only be opened if the VLANs are added to a team from the **Teaming Configuration** dialog box.

To display the **VLAN Statistics** dialog box for a team, use the following steps.

1. From the Ethernet port level, select an Ethernet port from the device tree.
2. Click **Statistics** on the **Teaming Configuration** dialog box.

   The **VLAN Statistics** dialog box displays.

Displaying VLAN statistics through BCU

Use the **team –vlanquery** command to display VLAN statistics for a team (Windows systems only).

```
team --vlanquery <team-name> <vlan_id>
```

where:

vlan_id	Specifies the VLAN identifier. The range for the VLAN ID is 1 to 4094.

VLAN statistics for a port (CNA and NIC)

Use the BCU **ethport** command to display VLAN statistics for a specific port, such as transmit and receive bytes, duration, and status.

```
ethport --vlanquery <pcifn> <vlan_id>
```

where:

pcifn	Specifies the PCIFN function number related to the port.
vlan_id	Specifies the VLAN identifier. The range for the VLAN ID is 1 to 4094.

Diagnostics

Diagnostics available through BCU commands and HCM evaluate the integrity of adapter hardware and end-to-end connectivity in the fabric. All of these diagnostics can be used while the system is running.

NOTE
Be sure to disable the port before running any type of port diagnostics.

NOTE
It is advisable to not perform other operations on the adapter while running HCM or BCU diagnostics.

Beaconing (stand-up adapters)

Initiate beaconing on a specific adapter port to flash the port LEDs and make it easier to locate the adapter in an equipment room.

Initiate link beaconing to flash the LEDs on a specific adapter port and the LEDs on a connected switch port to verify the connection between adapter and switch. When you initiate link beaconing, commands are sent to the other side of the link. When the remote port receives these commands, that port's LEDs flash. The remote port sends a command back to the originating port. When that port receives this command, the port's LEDs flash.

NOTE
To initiate link beaconing, this feature must be available on the connected switch.

Toggle beaconing on and off and set beaconing duration using the BCU or HCM.

Enabling beaconing through BCU

Use the **diag –beacon** command to enable beaconing for a specific adapter port.

```
diag --beacon <port_id> <on | off>
```

where:

port_id	ID of the port for which you want to enable beaconing. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

Use the **fcdiag –linkbeacon** command to enable end-to-end beaconing.

```
fcdiag --linkbeacon <portid> {on | off}
```

where:

port_id	ID of the port for which you want to run a link beacon test. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.
on | off	Toggle on or off. If turned on, you can specify duration.

Enabling beaconing through HCM

Enable link and port beaconing using the following steps.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Configure > Beacon**.
4. Click the **Link** check box, the **Port** check box, or both.

Internal and external loopback tests

Use the BCU or the HCM to perform a loopback test for a specific port. Loopback tests require that you disable the port. The following loopback tests are available:

- Internal

  Random data patterns are sent to the adapter port, then returned without transmitting through the port. The returned data is validated to determine port operation. Errors may indicate a failed port.

- External

  For this test, a loopback connector is required for the port. For mezzanine or expansion card adapters, this test can be performed using a pass-through module. Random data patterns are sent to the adapter port. The data transmits from the port and then returns. The returned data is validated to determine port operation. Errors may indicate a failed port.

Performing loopback tests through BCU

Use the **diag –loopback** BCU command test to verify port function through a loopback test.

```
bcu diag --loopback <port_id> [-t <loopback_type>][-s <speed>]
[-c <frame_count>] [-p <pattern>]
```

where:

port_id	ID of the port for which you want to run the test. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.
loopback type	Type of loopback test. Possible values are internal, external, and serdes.

speed	For HBAs and Fabric Adapter ports configured in HBA mode only. For a 4 Gbps port, this is 2 or 4. For an 8 Gbps port, this is 2, 4, or 8. For a 16 Gbps port, this is 4, 8, or 16.
frame count	Integer from 0 to 4,294,967,295. Default is 8192.
-p pattern	Hex number. Default value is A5A5A5A5.

Performing loopback tests through HCM

Use the **Hardware Tests** tab on the **Diagnostics** dialog box to perform a loopback test.

1. Launch the HCM.
2. Select **Configure > Diagnostics**.
3. Click the **Hardware Tests** tab.
4. Select **Loopback Test**.

   You can modify the following test parameters:

   - Subtest - The three options are Internal, Serdes, and External.
   - Link Speed (HBAs and Fabric Adapter ports configured in HBA mode) - For 16G ports, 4G, 8G, or 16G. For 8G ports, 2G, 4G, and 8G. For 4G ports, 1G, 2G, and 4G. For 4G ports, 2G and 4G.
   - Frame Count - Integer from 0 to 4,294,967,295. Default value is 8192.
   - Data Pattern - Hex value. Default value is A5A5A5A5.
5. Click **Start**.

Ethernet port loopback test (CNA)

Run Ethernet loopback tests on CNA ports and Fabric Adapter ports configured in CNA or NIC mode. Use BCU commands and HCM to test the Ethernet data path from the host to serdes or external loopback based on your selection. For mezzanine or expansion card adapters, this test can be performed using a pass-through module.You must disable the port before testing and use a loopback connector for the test.

NOTE
For 64-bit platforms only, you cannot perform Ethernet loopback tests on the port unless a VLAN is first created for the port.

Performing Ethernet loopback tests through HCM

Using the **Ethernet Tests** tab on the **Diagnostics** dialog box, you can run Ethernet loopback tests and set test parameters such as external subtests, serdes subtests, link speed, frame count, test cycle, and data pattern to test. Results display on the bottom of the tab as the test commences.

1. Launch the HCM.
2. Select **Configure > Diagnostics**.
3. Click the **Ethernet Tests** tab.
4. Select **eth Loopback Test**.

Performing Ethernet loopback tests through BCU

Refer to "Performing loopback tests through BCU" on page 90.

PCI loopback test

Use BCU commands or HCM to perform a PCI loopback test for a specific port. In this test, a data pattern is sent from the host to adapter firmware through the PCI bus. The returned data is validated to determine PCI operation.

NOTE
You must disable the port before you run loopback tests.

Performing PCI loopback tests through BCU

Use the **diag –pciloopback** BCU command to perform a PCI loopback test.

```
diag --pciloopback <port_id> [-p <pattern>] [-c <frame_count>]
```

where:

port_id	ID of the port from which you want to run the test. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.
pattern	Specifies the data test pattern. Must be at least one hexadecimal word.
frame count	Specifies the frame count as an integer from 0 to 4,294,967,295.

Performing PCI loopback tests through HCM

Use the **Hardware Tests** tab on the **Diagnostics** dialog box to perform a PCI loopback test as follows.

1. Launch the HCM.
2. Select **Configure > Diagnostics**.
3. Click the **Hardware Tests** tab.
4. Select **PCI Loopback Test**.

   You can modify the following parameters:

   - Frame count: Specifies the frame count as an integer from 0 to 4,294,967,295.
   - Data pattern: Specifies the data test pattern. Must be at least one hexadecimal word.
   - Test cycle: The number should be positive and the default is 1.
5. Click **Start**.

Memory test

Use the BCU or the HCM to perform a memory test for the adapter.

NOTE
Performing the memory test disables the adapter.

Performing a memory test through BCU

Use the **diag –memtest** command to test the adapter's memory blocks.

```
diag --memtest <ad_id>
```

where:

ad_id	ID of the adapter.

Performing a memory test through HCM

Use the **Hardware Tests** tab on the **Diagnostics** dialog box as follows to perform a memory test.

1. Launch the HCM.
2. Select **Configure > Diagnostics**.
3. Click the **Hardware Tests** tab.
4. Select **Memory Test**.
5. Specify the test cycle using a positive number.
6. Click **Start**.

Pinging Fibre Channel end points

Use the BCU and HCM to ping a Fibre Channel end point from an adapter port to determine the basic connectivity to the remote port and monitor network latency.

NOTE
Ping testing is not supported on Solaris systems.

Issuing a ping command to end points through BCU

Use the **fcdiag –fcping** BCU command to test the connection to a Fibre Channel end point.

```
fcdiag --fcping <port_id> <rpwwn> [-l <lpwwn>]
```

where:

port_id	ID of the adapter port from which you want to ping the remote port. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.
rpwwn	Remote PWWN that you want to ping.
lpwwn	Logical PWWN. 0 indicates the base port.

Issuing a ping command to end points through HCM

Use the **FC Protocol Tests** tab on the **Diagnostics** dialog box to test the connection to Fibre Channel end points. Use the following steps to ping end points.

1. Launch the HCM.
2. Select **Configure > Diagnostics** to display the **Diagnostics** dialog box.
3. Click the **FC Protocol Tests** tab.
4. Select **FC Ping Test**.
5. Select the adapter port and target that you wish to ping.
6. Enter a test cycle if applicable.
7. Click **Start**.

Adapter temperature

Use the BCU **diag –tempshow** command to read the adapter's temperature sensor registers.

```
diag --tempshow <ad_id>
```

where:

ad_id	ID of adapter.

Queue test

Use BCU commands and the HCM to send a health check message from the host to the firmware through message queues memory mapped over the PCI.

Performing a queue test through BCU

Use the **diag –queuetest** command to perform a queue test.

```
diag --queuetest <port_id> [-q <queue_num>]
```

where:

port_id	Adapter port number. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.
-q queue_number	Specifies the CPE queue number from 0 to 3. If the queue number is not specified, all queues are tested.

Performing a queue test through HCM

Use the **Hardware Tests** tab on the **Diagnostics** dialog box as follows to perform a queue test.

1. Launch HCM.
2. Select **Configure > Diagnostics.**
3. Click the **Hardware Tests** tab.

4. Select **Queue Test**.
5. Click **Start**.

SCSI test

Use the **fcdiag --scsitest** command to test SCSI components and display discovered LUN information, such as LUN number, device type and qualifier, vendor ID, product ID, revision number, size of LUN, and LUN status.

```
fcdiag --scsitest <port_id> <rpwwn> [-l <lpwwn>]
```

where:

port_id	ID of the port from that you want to test. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 use 1/1 as the port identification.
rpwwn	Remote PWWN to which you want to trace the route.
lpwwn	Logical PWWN. 0 indicates the base port or else the virtual port.

Trace route

Use the BCU and HCM to trace the SAN path between the adapter and remote end point.

Tracing the route through BCU

Use the **fcdiag --traceroute** BCU command to trace the route between end points.

```
fcdiag --fctraceroute <port_id> <rpwwn> [-l <lpwwn>]
```

where:

port_id	ID of the port from which you want to trace the route. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 use 1/1 as the port identification.
rpwwn	Remote PWWN to which you want to trace the route.
lpwwn	Logical PWWN. 0 indicates the base port.

Tracing the route through HCM

Use the FC Trace Route test to trace the route between the adapter port and a Fibre Channel target port. To run this test, use the following steps:

1. Launch the HCM.
2. Select **Configure > Diagnostics** to display the **Diagnostics** dialog box.
3. Click the **FC Protocol Tests** tab.
4. Select **FC Trace Route**.
5. Select the adapter port and target for which you wish to trace the route.

6. Enter a test cycle if desired.
7. Click **Start**.

Echo test

Use the BCU and HCM to initiate an echo test between the adapter port and a Fibre Channel end point. This sends an ECHO command and response sequence between the adapter port and target port to verify connection with the target.

Performing an echo test through BCU

Use the **fcdiag –fcecho** BCU command to initiate an echo test between the adapter and remote port.

```
fcdiag --fcecho <port_id> <rpwwn> [-l <lpwwn>]
```

where:

port_id	ID of the port that you want to test. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.
rpwwn	Remote port WWN to which the echo command is being sent.
lpwwn	Logical port WWN. 0 indicates the base port.

Performing an echo test through HCM

Use the Echo Test feature as follows to initiate an echo test between the adapter port and a Fibre Channel end point.

1. Launch the HCM.
2. Select **Configure > Diagnostics** to display the **Diagnostics** dialog box.
3. Click the **FC Protocol Tests** tab.
4. Select **Echo Test**.
5. Select the adapter port and target port for the test.
6. Enter a test cycle if applicable.
7. Click **Start**.

Collecting BIOS data

Collect information on the currently configured BIOS and boot over SAN configuration using the BCU and HCM.

Displaying BIOS data through BCU

Use the **bios –query** BCU command to display such information as the boot over SAN enabled or disabled state, port speed, boot LUNs obtained from flash, and boot LUNs obtained from the fabric (only if automatic discovery of boot LUNs from the fabric is enabled). Any “Preboot” output means that parameters were configured using a blade system management application. Preboot configuration data can include port speed, BIOS (boot over SAN) state, and configured boot LUN identification. Preboot data can also include the FCoE MAC, WWN, and VLAN and Ethernet MAC and VLAN information.

```
bios --query <port_id>
```

where:

port_id	The ID of the port for which you want to display the data. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

Display BIOS data through HCM

Display current BIOS information through the HCM Boot over SAN dialog box. Information includes BIOS (boot over SAN) enabled or disabled state, port speed, boot option, preboot BIOS enable and port speed, and details on current boot LUNs. To access this dialog box, use the following steps.

1. Select a host, an adapter, or an adapter’s physical port from the HCM device tree.
2. Select **Configure > Basic Port Configuration**.

   The **Basic Port Configuration** dialog box displays.
3. Click the **Boot-over-SAN** tab.

   The **Boot over SAN** dialog box displays.

Collecting LLDP data (CNA)

Collect information on the Link Layer Discovery Protocol (LLDP) associated with a specific CNA or a Fabric Adapter port configured in CNA mode using the HCM **LLDP Properties** panel.

The **LLDP Properties** panel displays information such as the MAC address of the local system, LLDP operational status, system management address, user-configured port description, port identification, configured name of local system, system capabilities based on system model, and time to live (TTL) values in LLDP frames.

To collect LLDP data, perform the following steps.

1. Select a CNA or Fabric Adapter in the device tree.
2. Click the **LLDP** tab in the right pane.

Collecting SFP data (stand-up adapters)

This section provides an overview of BCU commands and HCM features that provide information on small form factor pluggable (SFP) transceivers.

SFP properties

BCU and HCM provide detailed information on the SFP transceiver for a selected port, such as its health status, port speed, connector type, minimum and maximum distance, as well as details on the extended link.

Displaying SFP properties through BCU

Use the **diag –sfpshow** BCU command to display detailed attributes for a specific SFP transceiver.

```
diag --sfpshow <port_id>
```

where:

port_id — ID of the port for which you want to display SFP attributes. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

Initiating SFP properties through HCM

Launch the port **SFP** properties dialog box as follows to display properties for a selected small form-factor pluggable (SFP) transceiver.

1. Launch the HCM.
2. Select a port in the device tree.
3. Click the **SFP** tab in the right pane.

Predictive optical monitoring (POM)

Use the **POM** field in the port properties panel to monitor the SFP attributes. A notification is given for any parameters that are not within the power, temperature, voltage, and current specifications. To display this panel, use the following steps.

1. Select a port in the device tree.
2. Click the **Properties** tab in the right pane.

Collecting port data

This section provides an overview of BCU commands and HCM features that provide information on adapter ports. such as PWWN, node WWN, port type, configured speed, operating speed, configured topology, operating topology. link and port beaconing state, and other information.

Displaying port properties

Use the port **Properties** tab to display information about a selected base adapter port, such as the following:

- Port number
- PWWN and node WWN
- Factory PWWN and node WWN
- Port type (CNA or HBA)
- Media type (for example “mezz” for mezzanine)
- Current FCoE and factory MAC address (CNAs Fabric Adapter ports configured in CNA mode)
- Offline or online state
- Role of port (for example, FCP initiator)
- Fibre Channel address (HBAs and Fabric Adapter ports configured in HBA mode)
- WWN of the attached switch
- Operating topology (for example, point-to-point)
- Receive and transmit BB_Credits

NOTE
“Mezz” for the media type indicates “mezzanine.” The “Pre-Boot” identification for certain properties means that the property was configured using a blade system management application.

Use the following steps to display base port properties.

1. From the device tree, select a base port.
2. Click the **Base Port Properties** tab in the right pane.

Displaying DCB port properties (CNA)

Use the **DCB Port Properties** panel to display information for a selected DCB adapter port on a CNA or Fabric Adapter with a port configured in CNA mode.

Information such as the following displays:

- DCB status
- FCoE logical link status
- DCBCXP version
- Network priority configuration
- Network priority group ID
- Bandwidth percentage for given port group
- Priority flow control status

- FCoE quality of service that specifies a priority value

To display DCB port properties, use the following steps.

1. Select a DCB port in the device tree.
2. Click the **Properties** tab in the right pane.

Displaying Ethernet port properties (CNA or NIC)

You can display Ethernet properties for CNA ports or Fabric Adapter ports configured in CNA or NIC mode using the HCM **Ethernet Port Properties** panel.

Information such as the following displays:

- Name of Ethernet device
- Port type
- Current (FCoE) and factory MAC address
- IOC identification
- WWN of hardware
- Status of port, such as linkup
- Ethernet logging level

To display Ethernet port properties, use the following steps.

1. Select an Ethernet port in the device tree.
2. Click the **Properties** tab in the right pane.

Displaying FCoE port properties (CNA)

Use the HCM **FCoE Port Properties** to display FCoE port properties for CNAs or Fabric Adapter ports configured in CNA mode. Properties include the following:

- Current FCoE MAC address
- Supported class
- FC frame size
- Maximum transmission unit (MTU)
- Target rate limiting (TRL) enabled or disabled status
- Default rate limit
- Beaconing status
- Fibre Channel Initialization Protocol (FCIP) operational state
- Local (factory) port MAC address
- Fibre Channel address
- Priority group ID (PGID)
- Queue depth
- Interrupt control delay
- Bandwidth percentage for priority group
- MAC address for FCoE forwarder

- Fabric WWN
- Fibre Channel map ID
- FCoE forwarder writing or nonwriting mode
- Maximum speed supported
- Port operating topology
- Authentication status, algorithm, group, and error status

Displaying FCoE port properties

To display the HCM **FCoE Port Properties** panel, use these steps.

1. Select an FCoE port in the device tree.
2. Click the **Properties** tab in the right pane.

Displaying FC port properties (HBA)

Use HCM **vHBA Properties** to display FC port properties for HBAs or Fabric Adapter ports configured in HBA mode. Properties include the following:

- Port WWN
- Node WWN
- Path TOV (not displayed for Solaris systems)
- Port log
- I/O profile

To display the HCM **vHBA Port Properties** panel, use these steps.

1. Select an FC port in the device tree.
2. Click the **vHBA** tab in the right pane.

Displaying remote port properties

Use the HCM **Remote Port Properties** panel to display properties that are associated with the remote port, such as WWN, node WWN, port name, Fibre Channel address, frame data field size, online or offline state, role (such as target or initiator), remote device information, QoS priority, QoS flow, and target ID. Display this properties panel using the following steps.

1. From the device tree, select a remote port.
2. Click the **Remote Port Properties** tab in the right panel.

   If it is a target port, two tabs display in the right pane: **Properties** and **LUNs**.

Displaying logical port properties

Use the HCM **LPorts Properties** panel to display properties associated with a logical port, such as port and node WWN, Fibre Channel address, online or offline state, fabric name, and name server activity. To display logical port properties, use the following steps.

1. From the device tree, select a logical port.
2. Click the **LPORTs Properties** tab in the right panel.

Displaying virtual port properties

Use the HCM **Virtual Port Parameters** properties panel to display the properties associated with a virtual port, such as PWWN and node WWN, Fibre Channel address, offline or online state, role (such as FCP initiator), and attached switch WWN. For mezzanine or expansion card adapters, "pre-boot" display indicates that virtual port configuration was accomplished using a blade system management application.

To display virtual port properties, use the following steps.

1. From the device tree, select a virtual port.
2. The **Virtual Port Parameters** properties panel displays.

Displaying the port log

Use the **debug –portlog** BCU command to display a log of Fibre Channel frames and other main control messages that were sent out and received on a specific port. You can use this information to isolate adapter and Fibre Channel protocol problems.

```
debug --portlog <port_id>
```

where:

port_id — The ID of the port for which you want to display the port log. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

NOTE
If the port log is disabled, a warning message displays. Use the **debug -portlogctl** command to enable and disable the port log.

Displaying the port list

Use the **port –list** BCU command to list all physical ports on the adapter along with their physical attributes, such as PWWN, media type, Fibre Channel address, port type, trunking state, speed, operating state, loopback mode state, and diagnostics state. For CNAs and Fabric Adapter ports configured in CNA mode, output also includes Ethernet and DCB link states. For mezzanine or expansion card adapters only, a # symbol next a “disabled” state indicates that the port was disabled using a blade system management application. A “pre-boot” display indicates that virtual port configuration was accomplished using a blade system management application. The media entry will be “mz” to indicate mezzanine card.

```
port --list [<-verbose | -terse>]
```

Performing a port query

Use **port –query** BCU command to display information, such as port name, state, current and configured speed, topology, media type, received and transmitted BB_Credits, beacon status, QoS priority status, QoS flow identification, port binding status, beaconing status, target rate limiting (TRL) status, and TRL default speed. Other information includes FCoE attributes, such as the current PWWN and NWWN, factory PWWN and NWWN, current and factory MAC address, link state, as well as Ethernet attributes, such as the current and factory MAC address, current and factory VLAN values, and link state.

For mezzanine or expansion card adapters, a # symbol next a “disabled” state indicates the port was disabled using a blade system management application. A “pre-boot” display indicates that virtual port configuration was accomplished using a blade system management application. The media entry will be “mz” to indicate mezzanine card.

```
port --query <port_id>
```

port_id — ID of the port for which you want to display information. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

Displaying port speed

Use **port –speed** BCU command to display the current port speed setting.

```
port --speed <port_id>
```

where:

port_id — ID of the port for which you want to display port speed. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

FCP-IM I/O profiling

This feature, available through BCU commands and HCM, can be enabled or disabled on a physical port. When enabled, the driver firmware categories I/O latency data into average, minimum, and maximum categories. Use this feature to analyze traffic patterns and help tune adapters, fabrics, and targets for better performance. Note that enabling this feature impacts I/O performance. View this information in the **Port Statistics** window.

Enabling FCP-IM profile through HCM

1. Select an FC or FCOE port from the HCM device tree.
2. Select **Configure > vHBA Configuration**.

   The **vHBA Configuration** dialog box displays.
3. Click the **FCP-IM IO profile on** checkbox.

   Adding a check mark enables profiling. Removing the check mark disables profiling.

Enabling FCP-IM profile through BCU

Use **fcpim –profile** commands to enable or disable profiling.
To enable I/O profiling, use the following command.

```
fcpim --profile_on
```

To disable I/O profiling, use the following command.

```
fcpim --profile_off
```

where:

port_id — ID of the port for which you want to enable or disable I/O profiling. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

Collecting teaming information (CNA or NIC)

Use the Brocade CLI utility (BCU) or HCM to display information on teaming for CNAs or Fabric Adapter ports configured in CNA or NIC mode.

NOTE
Teaming commands apply to Windows operating systems only.

Displaying team data and statistics through HCM

Use the **Teaming Configuration** dialog box to display the team name, members, mode, MAC address, time delay, transmit policy, and active link for a selected team. You can also display teaming statistics for a selected team, such as transmit and receive bytes, connection status, and connection duration. Use the following steps to display this dialog box.

1. Select a local host icon from the device tree in Host Connectivity Manager (HCM).
2. Select **Configure > Teaming**.

   OR

   Right-click the local host icon and select **Teaming**.

   The **Teaming Configuration** dialog box displays.
3. Select a team from the **Teams** list to display properties for the team.
4. Click the **Statistics** button beneath the **Teams** field to display statistics for the selected team.

Display teaming statistics for all configured teams using the following steps.

1. Select a local host icon from the device tree.
2. Right-click the local host icon and select **Statistics > Teaming Statistics**.

   Statistics display for all teams configured on the host.

Displaying configured team data through BCU

Use the **bcu team –list** and **bcu team –query** commands to display information about configured teams. Following is an overview of both commands:

- The **bcu team –list** command displays all configured teams by their configured IDs, the team mode (failback, failover, or 902.3ad), and the team's MAC address.

  ```
  team --list
  ```

- The **bcu team –query** command displays the teaming configuration for a specific team including the team mode, MAC address, and number of ports. Also included are statistics, such as transmit and receive bytes, connection status, and connection duration.

  ```
  team --query <team-name>
  ```

  where:

  team-name ID of the team for which you want to display information.

Authentication settings

Use the BCU or HCM to display the adapter authentication settings and status.

Displaying authentication settings through HCM

Launch the **Fibre Channel Security Protocol Configuration** dialog box as follows to display authentication settings.

1. Right-click an adapter and select **Authentication** from the list. from the device tree.

   The **Fibre Channel Security Protocol Configuration** dialog box displays. This displays the current CHAP secret, hashing algorithm, and group value.

Displaying authentication settings through BCU

Use the BCU **auth –show** command to display authentication settings.

```
auth --show <port_id>
```

where:

port_id	ID of the port for which you want to display authentication settings. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1, you would use 1/1 as the port identification.

PHY module data

The Ethernet PHY module, located in the mezzanine card port hardware, aids in communications to and from the Ethernet LAN. Use the **bcu phy –query** command to query the PHY module and determine attributes, such as the PHY module status, installed firmware version, link partner auto-negotiation ability, PHY auto-negotiation ability, PMA (physical medium attachment sublayer) and PMD (physical medium dependent sublayer) link status and signal detected, and PCS (physical coding sublayer) link status.

```
bcu phy --query <port_id>
```

where:

<port_id>	ID of port for which you want to display data. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

QoS settings (HBA)

Display Quality of Service (QoS) settings on HBAs and Fabric Adapter ports configured in HBA mode. QoS works in conjunction with the QoS feature on Brocade switches to assign traffic priority (high, medium (default), low) to a given source and destination traffic flow.

Determining QoS settings through BCU

Use the following commands to deter ming QoS settings:

- Use the following BCU command to display QoS enabled status.

  ```
  port --query <port-id>
  ```

  where:

port_id	ID of the port for which you want to display settings.

- Use the following command to display QoS status and other information for a port.

  ```
  qos --query <port_id>
  ```

  where:

port_id	ID of the port for which you want to display settings.

- Use the following command to determine operating speed of the remote port and QoS status.

  ```
  rport --query <port_id> <rpwwn> [-l <lpwwn>]
  ```

  where:

port_id	Specifies the ID of the port for which you want to query attributes of a remote port.
rpwwn	Remote PWWN. You can obtain the RPWWN from the BCU rport –list <port_id> command.
-l lpwwn	Logical PWWN. This is an optional argument. If the -l lpwwn argument is not specified, the base port is used.

Determining QoS settings through HCM

Use HCM in the following ways to determine current status and configuration for QoS:

- Use the **Port Properties** panel in HCM to display configured QoS parameters.
  1. Select a port in the device tree.
  2. Click the **Properties** tab in the right pane.

     The **Port Properties** panel displays
- Use the **Remote Port Properties** panel in HCM to display information on QoS for the remote port.
  1. From the device tree, select a remote port (target or initiator).
  2. Click the **Remote Port Properties** tab in the right pane.

     The **Remote Port Properties** panel displays.

Target rate limiting settings (HBA)

Display target rate limiting settings on HBA ports or Fabric Adapter ports configured in HBA mode. Target rate limiting throttles the Fibre Channel Protocol (FCP) read traffic rate to slow-draining targets to reduce or eliminate network congestion and alleviate I/O slowdowns to faster targets.

Use the following BCU commands to determine current status and configuration for target rate limiting settings:

Determining target rate limiting settings through BCU

Use the following BCU commands to determine current status and configuration for target rate limiting settings:

- Use the following BCU command to determine target rate limiting speed and enabled status.

  ```
  ratelim --query <port-id>
  ```

  where:

port_id — ID of the port for which you want to display target rate limiting settings. This could be the PWWN, port hardware path, or user-specified port name. This could also be the adapter-index/port-index. For example, to specify adapter 1, port 1 you would use 1/1 as the port identification.

- Use the following BCU command to display target rate limiting enabled status and default speed.

  ```
  port --query <port-id>
  ```

  where:

  port_id — ID of the port for which you want to display port information.

- Use the following command to determine operating speed of the remote port and target rate limiting enforcement.

  ```
  rport --query <port_id> <rpwwn> [-l <lpwwn>]
  ```

  where:

  port_id — Specifies the ID of the port for which you want to query attributes.

  rpwwn — Remote PWWN. You can obtain the RPWWN from the BCU rport –list <port_id> command.

  -l lpwwn — Logical PWWN. This is an optional argument. If the -l lpwwn argument is not specified, the base port is used.

Determining settings through HCM

Launch the **Remote Port Properties** panel in HCM as follows to display information on target rate limiting and QoS for the remote port.

1. From the device tree, select a remote port (target or initiator).
2. Click the **Remote Port Properties** tab in the right pane.

   The **Remote Port Properties** panel displays.

Persistent binding

Persistent binding is a feature of adapters that enables you to permanently assign a system SCSI target ID to a specific Fibre Channel (FC) device, even though the device's ID on the FC loop may be different each time the FC loop initializes. Persistent binding is available in the Windows and VMware environments only.

Use HCM features or BCU commands to display target ID mapping for an adapter port.

Displaying Persistent Binding settings through BCU

Use the **pbind –list** BCU command to query the list of mappings for persistent binding on a specific port.

```
pbind --list <port_id> <pwwn>
```

where:

port_id	ID of the port for which you want to display settings.
pwwn	Port World Wide Name

Displaying Persistent Binding settings through HCM

Launch the **Persistent Binding** dialog box as follows to determine SCSI target ID mappings:

1. Launch the HCM.
2. Select an adapter, host, DCB port, or FCoE port from the device tree.
3. Launch
4. Select **Configure > Persistent Binding. > View Persistent Binding.**

Adapter properties

Display properties for the following using HCM:

- CNAs or Fabric Adapter ports configured in CNA mode.
- HBAs or Fabric Adapter ports configured in HBA mode.

CNA Properties

Following are the some of the properties that you can display for CNAs or Fabric Adapter ports configured in CNA mode:

- MAC address
- Adapter name
- Operating status
- Vendor ID
- PCIe generation
- Subsystem vendor ID
- Serial number
- Manufacturer
- Model description
- Maximum speed supported
- Number of ports
- OEM information
- Card type

- Hardware Path
- Serial number
- Temperature
- Driver Version
- Driver name
- Firmware version
- BIOS version

To display the properties panel, perform the following steps:

1. Select a CNA or Fabric Adapter port configured in CNA mode
2. Click the **Properties** tab in the right pane.

HBA Properties

Following are some of the properties that you can display for HBAs or Fabric Adapter ports configured in HBA mode:

- Node WWN
- Adapter name
- Operating status
- Manufacturer
- Model description
- Maximum speed supported
- Number of ports
- OEM information
- Card type
- Chip revision
- Trunking supported
- Junction temperature
- Driver name, version
- Firmware version
- BIOS version
- Subsystem vendor ID
- Number of PCI lanes
- PCIe generation

To display the properties panel, perform the following steps:

1. Select an HBA or Fabric Adapter port configured in HBA mode
2. Click the **Properties** tab in the right pane.

Adapter queries

Use BCU commands to list and query available adapters seen by the driver.

The **bcu adapter –list** command lists all adapters on the system with a brief summary of information such as model number, serial number, and adapter number. Enter the following command:

```
adapter --list
```

where:

list	Lists all adapters in the system. For each adapter in the system, a brief information line displays containing the adapter type, model number, serial number, and hardware path.

The **adapter –query** command displays adapter information, such as the current version of the adapter, adapter type, adapter (chip revision) and driver (fw version), maximum port speed, model information, serial number, number of ports, PCIe information, pwwn, nwwn, hardware path, flash information (such as firmware version), BIOS version, EFI version, current power mode, and port information (PWWN, NWWN, beacon status).

```
adapter --query <ad_id>
```

where:

ad_id	ID of the adapter for which you want to query.

Chapter

4

Performance Optimization

In this chapter

- Tuning storage drivers 113
- Tuning network drivers (CNA or NIC) 116

Tuning storage drivers

This section provides resources for optimizing performance in adapters by tuning the unified storage drivers on Linux, Windows, Solaris, and VMware systems. To optimize performance for CNAs and Fabric Adapter ports configured in CNA or NIC mode, also use resources under "Tuning network drivers (CNA or NIC)" on page 116.

Linux tuning

Linux disk I/O scheduling reorders, delays, and merges requests to achieve better throughput and lower latency than would happen if all the requests were sent straight to the disk. Linux 2.6 has four different disk I/O schedulers: noop, deadline, anticipatory and completely fair queuing. Enabling the "noop" scheduler avoids any delays in queuing of I/O commands. This helps in achieving higher I/O rates by queuing multiple outstanding I/O requests to each disk.

To enable the noop scheduler, run the following commands on your system.

```
for i in /sys/block/sd[b-z]/queue/scheduler
do
echo noop > $i
done
```

NOTE
You must disable the default scheduler because it is not tuned for achieving the maximum I/O performance.

For performance tuning on Linux, refer to the following publications:

- *Workload Dependent Performance Evaluation of the Linux 2.6 IO Schedulers*
  Heger, D., Pratt, S., Linux Symposium, Ottawa, Canada, July 2004
- *Optimizing Linux Performance*
  HP Professional Books, ISBN: 0-13-148682-9
- *Performance Tuning for Linux Servers*
  Sandra K. Johnson, Gerrit Huizenga, Badari Pulavarty, IBM Press, ISBN: 013144753X
- *Linux Kernel Development*

Robert Love, 2nd edition, 2005

Solaris tuning

To increase I/O transfer performance, set the following parameters on your system:

- Set the maximum device read/write directive (maxphy).
- Set the disk maximum transfer parameter (ssd_max_xfer_size).

Please refer to the *Sun StorageTek SAM File System Configuration and Administration Guide* document for details of the two parameters.

To increase I/O write performance, set the pcie-max-read-reqsz parameter on your system. This parameter is defined in /kernel/drv/bfa.conf. It determines the maximum read through PCIe. The default value is 512. To increase performance, you can increase the value to 256, 1024, or 2048.

NOTE
Brocade 804 and 1007 adapters are not supported on Solaris systems so Solaris commands do not apply to these adapters.

Windows tuning

Windows tuning involves configuring the driver and operating system tunable parameters.

Driver tunable parameters

You can manipulate several driver parameters to increase performance.

bfa_lun_queue_depth (outstanding I/O requests per LUN)

The driver uses a default LUN queue depth value of 32. This value is chosen to reflect the average operating I/O load in most scenarios. Storport manages the I/O throttling at the per-LUN level to guarantee the configured queue depth. During performance testing with specific high-end array LUNs, it may be necessary to increase this I/O queue depth to a much larger value. Microsoft recommends a value of 96 during high-performance testing scenarios. If the queue depth is not sufficient, then you will notice performance degradation.

The queue depth can be configured at the following registry location with any value within the range 1 through 254.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bfad\Parameters\Device\bfa_lun_queue_depth

Interrupt moderation using interrupt coalescing feature

Moderating interrupts can often result in reduced CPU load on the host but, unless interrupt moderation is performed intelligently, the CPU savings might increase latency.

The default values for the Fibre Channel port interrupt attributes are configured as follows:

- Interrupt coalescing

  Default: ON

- Interrupt delay

  Default:

  - 1125 microseconds on the Brocade 415, 425, 815, 825, and 1860
  - 25 microseconds on the Brocade 804, 1007, 1010, 1020, and 1741

  Valid Range: 0 through 1125 microseconds
  Note that the value of 0 disables the delay timeout interrupt.

- Interrupt latency

  Default:

  - 225 microseconds on the Brocade 415, 425, 815, 825, and 1860
  - 5 microseconds on the Brocade 804, 1007, 1010, 1020, and 1741

  Valid Range: 0 through 225 microseconds
  Note that the value of 0 disables the latency monitor timeout interrupt.

- Interrupt Coalescing

  When this feature is turned off, I/O completion requests are not coalesced by the firmware. While this helps reduce I/O latency, the host CPU will frequently be interrupted, leading to a slower system response under heavy I/O load (more than 7000 I/Os per second).

  When this feature is turned on, the adapter will not interrupt the host until **Interrupt delay** duration. **Interrupt delay**, together with **Interrupt latency**, helps to reduce the number of interrupts that the host CPU processes per second, leading to improved overall CPU utilization. However, if the number of interrupts handled between the **Interrupt delay** period is relatively smaller, then this will result in performance degradation as the I/O completion process has slowed down.

  The BCU **vhba** command can be used to configure these interrupt attributes for the desired port.

  ```
  vhba --intr pcifn <-c> {on | off} [<Latency> <Delay>]
  ```

Message signaled interrupts (MSI-X)

All Brocade adapters support MSI-X, an eXtended version of the MSI defined in PCI 3.0 specification. MSI-X helps improve overall system performance by contributing to lower interrupt latency and improved host CPU utilization.

MSI-X is supported in Windows Vista and Windows Server 2008.

To enable MSI-X, set the following registry key value to 0.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bfad\Parameters\Device\msix_
disable
```

OS tunable parameters

Please see the section “Storage Stack Drivers” in *Disk Subsystem Performance Analysis for Windows Server 2003 optimizations* located on the following website.

http://download.microsoft.com

Please see the sections “Performance Tuning for Storage Subsystem” and “I/O Priorities” in *Performance Tuning Guidelines for Windows Server 2008* located on the following website.

http://www.microsoft.com

VMware tuning

For performance tuning on VMware, refer to the following publications on the VMware website at www.vmware.com:

- *Performance Tuning Best Practices for ESX Server 3*. Refer to the following sections:
  - Storage Performance Best Practices
  - Related Publications
- *Fibre Channel SAN Configuration Guide*. Refer to "Using ESX Server with SAN: Concepts."

Tuning network drivers (CNA or NIC)

This section provides resources for tuning network drivers for CNAs or Fabric Adapter ports configured in CNA or NIC mode on Linux, Windows, and VMware systems. Note that the default values set for the driver parameters discussed in this section should provide optimum performance. However, you may need to modify these values depending on your network environment. Please follow your host and operating system guidelines when doing so.

Windows tuning

All Windows tunable parameters for the network driver are optimized for best performance using default values. For details on parameters in the following table, refer to the "Adapter Configuration" appendix in the *Brocade Adapters Installation and Reference Manual*. Table 9 provides default parameters for Windows tunable parameters.

TABLE 9 Default values for Windows tunable parameters

Parameter	Default
Log Level	3
Interrupt Moderation (Set for receive interrupts)	On
Jumbo Packet Size	9,000 bytes
TCP-UDP Checksum Offload	Enabled
Network Address	N/A
Priority and VLAN	Disabled
Receive Side Scaling (RSS)	Enabled
Large Segmentation Offload V1 IPv4 (LSOv1)	Enabled
Large Segmentation Offload V2 IPv4 (LSOv2)	Enabled
Large Segmentation Offload V2 IPv6 (LSOv2)	Enabled
FlowControl, Transmit (Tx) and Receive (Rx)	Enabled

TABLE 9 Default values for Windows tunable parameters

Parameter	Default
Interrupt Moderation	Enabled
VLAN ID	Disabled
Priority and VLAN Support	Enabled

Linux tuning

All Linux tunable parameters for the network driver are optimized for best performance using default values. For details on configuring the parameters in the following table, refer to the "Adapter Configuration" appendix in the *Brocade Adapters Installation and Reference Manual*. Table 10 provides default values for all Linux tunable parameters.

TABLE 10 Default values for Linux tunable parameters

Parameter	Default
Interrupt moderation	Enabled
Log Level	3
Jumbo packet size	9,000 bytes
TCP=UDP checksum offload	Enabled
TCP Segmentation Offload (TSO)	Enabled
MSI-X (Message Signaled Interrupts Extended	Enabled

VMware tuning

All VMware tunable parameters for the network driver are optimized for best performance using default values. For details on configuring the parameters in the following table, refer to the "Adapter Configuration" appendix in the *Brocade Adapters Installation and Reference Manual*. Table 11 provides default values for VMware tunable parameters.

TABLE 11 Default values for VMware tunable parameters

Parameter	Default
Jumbo Packet Size	9,000 bytes
VLAN ID	Disabled
MSI-X (Message Signaled Interrupts Extended)	Enable
Interrupt Moderation (Set for receive interrupts)	On
NetQueue	Disabled

Jumbo packet size

Recommendations to enhance performance

Increase throughput by setting MTU to 9000 bytes.

How to change values

Refer to instructions for Windows “network driver parameters” in “Adapter Configuration” appendix of the *Brocade Adapters Installation and Reference Manual*.

References for more tuning information

Refer to the *10Gbps Networking Performance on ESX 3.5 Update 1* available through www.vmware.com.

NetQueue

NetQueue improves receive-side networking performance on servers in 10 Gigabit Ethernet virtualized environments. NetQueue provides multiple receive queues on the CNA or Fabric Adapter port configured in CNA mode, which allows processing on multiple CPUs to improve network performance.

MSI-X is an eXtended version of Message Signaled Interrupts defined in the PCI 3.0 specification. All Brocade adapters support MSI-X, which helps improve overall system performance by contributing to lower interrupt latency and improved host CPU utilization. MSI-X is enabled by default in VMware ESX Server, and must remain enabled for NetQueue to function. Please make sure that bnad_msix=0 is not listed in VMware module parameters because that would disable NetQueue.

For the Brocade driver, you cannot directly configure the number of NetQueue and filters per NetQueue. By default, these values are based on the number of receive queue sets used, which is calculated from the number of CPUs in the system.

Default value: Disable

Possible values: Enable, Disable

Recommendations to enhance performance

Enabling NetQueue utilizes multiple receive queues of the Brocade adapter, which can be handled by multiple CPUs on the host system, thus improving performance.

How to change values

Refer to instructions for Windows “network driver parameters” in “Adapter Configuration” appendix of the *Brocade Adapters Installation and Reference Manual*.

References for more tuning information

Refer to the *10Gbps Networking Performance on ESX 3.5 Update 1* available through www.vmware.com.

Solaris tuning

All Solaris tunable parameters for the network driver are optimized for best performance using default values. For details, refer to the “Adapter Configuration” appendix in the *Brocade Adapters Installation and Reference Manual*.

For Solaris 10, you can enable support for jumbo packet frames and set the MTU size for these frames from 1,500 (default) to 9,000 bytes.

Appendix

Adapter BIOS and Event Message Reference A

This appendix provides details on BIOS messages that display during operation of option ROM and event messages that display during operation of adapter drivers. Included in these details are the message, cause, and action the user should perform after viewing these messages.

Adapter BIOS messages

Table 12 provides details on BIOS-related messages generated during operation of option ROM. The message, possible cause, and user action are provided.

TABLE 12 Adapter BIOS messages

Message	Cause	Recommended Action
Adapter<no> : No firmware present. Skipping card	There is no boot firmware present on the card.	Download the latest boot code file for installed Brocade adapters from your adapter's website. The boot code file is designated as: brocade_adapter_boot_fw_v<x.y.z> where x.y.z is the version number. Update boot code on all the adapters in the system using instructions in the "Boot Code" chapter of the *Brocade Adapters Installation and Reference Manual*.
Adapter<no> : Version mismatch: Card Ver<XXX>. Disabling BIOS	Current executing option ROM version is different from the one on the adapter.	Download the latest boot code file for installed Brocade adapters from your Brocade adapter's website. The boot code file is designated as: brocade_adapter_boot_fw_v<x.y.z> where x.y.z is the version number. Update boot code on all the adapters in the system using instructions in the "Boot Code" chapter of the *Brocade Adapters Installation and Reference Manual*.
Adapter<no> : No boot devices. Disabling BIOS	BIOS on this adapter is enabled, however no boot devices are configured.	If booting from this adapter is not required, then ignore this message. If booting from this adapter is required, perform the following steps: 1 Check if boot devices are configured through the Brocade BIOS Configuration Utility. If not, configure devices and try booting again. 2 In the zoning information on the switch, verify if the target's WWN are in the same zone as that of initiator's WWN.

TABLE 12 Adapter BIOS messages (continued)

Message	Cause	Recommended Action
Failed:<Disk: PWWN<Target's PWWN> LUN<LUN Id>. Adapter<no>	This adapter is unable to connect to the configured boot device. This error message is displayed only when boot option is set to **Flash Values** through the Brocade BIOS Configuration Utility.	1 Check the zoning information on the switch and verify if the target's WWN is in the same zone as the initiator's WWN. 2 Check that there is path configured between the initiator and the target boot device.
Adapter<no> : BIOS is disabled	BIOS is disabled for this adapter.	If booting through this adapter is desired, then launch the Brocade BIOS Configuration Utility by pressing Ctrl-B or Alt-B, then enable BIOS on the adapter port where connection is required.
Adapter<no> : Link initialization failed. Disabling BIOS	Unable to bring up the link for this adapter.	Check connectivity between the adapter port and the switch.
Boot device discovery failed. Disabling BIOS.	The boot option is set to **Fabric Discovered** or **First LUN** through the Brocade BIOS Configuration Utility, and the adapter is unable to discover any boot device.	If booting through this adapter is not desired, then ignore this message. If booting through this adapter is desired: 1 Launch the Brocade BIOS Configuration Utility by pressing Ctrl-B or Alt-B. 2 For the desired port, select **Auto Discover** for the **Boot LUN** field in the **Adapter Settings** menu. 3 Check if any boot devices are visible. If none are visible, then connect a boot device and repeat step 2. You should see the target and LUN information displayed during the discovery process.
Brocade BIOS installed successfully	This message displays if any adapters in the system are able to connect to a boot device.	None.

Adapter driver event messages

Table 13 provides details on event messages generated by adapter drivers. These events display in host system logs and the HCM master log. Events are organized as originating from the network driver only, storage driver only, or network and storage driver.

TABLE 13 Driver event messages

Message	Severity	Event Type	Category	Sub Category	Cause	Action
Network Driver Events (CNAS only)						
Base port link up: Hardware Address = [Base port MAC].	Information	Network driver	10 (EthPort)	Up	Base port Ethernet link is up.	No action required.
Base port link down: Hardware Address = [Base port MAC].	Warning	Network driver	10 (EthPort)	Down	Base port Ethernet link is down.	No action required.
Base port Ethernet Link is enabled: Hardware Address = [Base port MAC].	Information	Network driver	10 (EthPort)	Enabled	Ethernet port enabled by user.	No action required.

TABLE 13 Driver event messages (continued)

Message	Severity	Event Type	Category	Sub Category	Cause	Action
Base port link is disabled: Hardware Address = [Base port MAC].	Warning	Network driver	10 (EthPort)	Disabled	Ethernet port disabled by the user.	No action required.
Storage Driver Events						
Authentication enabled for base port: WWN = [Base port WWN].	Information	Storage driver	8 (AUDIT)	Enabled	Authentication enabled by user command.	No action required.
Authentication disabled for base port: WWN = [Base port WWN].	Information	Storage driver	8 (AUDIT)	Disabled	Authentication disabled by user command.	No action required.
Fabric name changed for base port: WWN = [Base port WWN].	Warning	Storage driver	2 (PORT)	Changed	Fabric name changed for base port.	No action required.
Logical port WWN: [logical port WWN], Role: [initiator, target, IPFC mode etc.] is deleted.	Information	Storage driver	3 (LPORT)	Deleted	Logical port deleted.	No action required.
Logical port online: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Online	Logical port (base or logical) logged into fabric.	No action required.
Logical port taken offline: WWN = WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Offline	Logical port (base or logical) logged out of fabric.	No action required.
Logical port lost fabric connectivity: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Error	Storage driver	3 (LPORT)	Offline	Logical port (base or logical) lost fabric connectivity.	Check switch and adapter configuration.
New logical port created: WWN = [logical port WWN], Role = [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Created	New logical port created.	No action required.
New virtual port created using proprietary interface: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Created.	New virtual port created.	No action required.
New virtual port created using standard interface: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Created	New virtual port created.	No action required.
QOS priority changed to [New QOS flow ID]: RPWWN = [Remote port WWN] and LPWWN = [Logical port WWN].	Information	Storage driver	4 (RPORT)	Changed	QOS priority changed.	No action required.
QOS flow ID changed to [New QOS flow ID]: RPWWN = [Remote port WWN] and LPWWN = [Logical port WWN].	Information	Storage driver	4 (RPORT)	Changed	QOS flow ID changed.	No action required.
Remote port (WWN = [remote port WWN] online for logical port (WWN = [logical port WWN]).	Information	Storage driver	4 (RPORT)	Online	Login nexus established with remote port.	No action required.

TABLE 13 Driver event messages (continued)

Message	Severity	Event Type	Category	Sub Category	Cause	Action
Remote port (WWN = [remote port WWN]) offlined by logical port (WWN = [logical port WWN]).	Information	Storage driver	4 (RPORT)	Offline	Login nexus with remote port terminated by logical port.	No action required.
Remote port (WWN = [remote port WWN]) connectivity lost for logical port (WWN = [logical port WWN]).	Error	Storage driver	4 (RPORT)	Offline	Login nexus with remote port is lost.	Check if remote port is having issues.
Target (WWN = [Target WWN]) is online for initiator (WWN = [Initiator WWN]).	Information	Storage driver	5 (ITNIM)	Online	SCSI IT-Nexus established between initiator and target.	No action required.
Target (WWN = [Target WWN]) offlined by initiator (WWN = [Initiator WWN]).	Information	Storage driver	5 (ITNIM)	Offline	SCSI IT-Nexus terminated by Initiator.	No action required.
Target (WWN = [Target WWN]) connectivity lost for initiator (WWN = [Initiator WWN]).	Error	Storage driver	5 (ITNIM)	Offline	SCSI IT-Nexus terminated between initiator and target.	No action required.
Virtual port deleted using proprietary interface: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Deleted	Virtual port deleted.	No action required.
Virtual port deleted using standard interface: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Deleted	Virtual port deleted.	No action required.
Virtual port login failed. Duplicate WWN = [logical port WWN] reported by fabric.	Warning	Storage driver	3 (LPORT)	Failed	Duplicate WWN reported by fabric.	Delete this vport and create with a different WWN.
Virtual port (WWN = [logical port WWN]) login failed. Max NPIV ports already exist in fabric/fport.	Warning	Storage driver	3 (LPORT)	Failed	Max NPIV ports already exist in fabric/fport.	Check fabric and fport configuration
Virtual port (WWN = %s) login failed.	Warning	Storage driver	3 (LPORT)	Failed	Unknown error.	Check fabric/fport configuration.
Network and Storage Driver Events						
Adapter removed: SN = [adapter serial number].	Warning	Network and storage driver	1 (Adapter)	Removed	Adapter removed.	Check PCIe connector and configuration.
Authentication successful for base port: WWN = [base port WWN or MAC].	Information	Network and storage driver	2 (Port)	Successful	Authentication successful.	No action required.

TABLE 13 Driver event messages (continued)

Message	Severity	Event Type	Category	Sub Category	Cause	Action
Authentication unsuccessful for base port: WWN = [base port WWN or MAC].	Error	Network and storage driver	2 (Port)	Failure	Authentication failure.	Mismatch of FC-SP configuration between switch and HBA. Also, check the authentication secret setting.
Base port enabled: Hardware Address = [base port WWN or MAC].	Information	Network and storage driver	2 (Port)	Enabled	Base port enabled by user command.	No action required.
Base port disabled: Hardware Address = [base port WWN or MAC].	Warning	Network and storage driver	2 (Port)	Disabled	Base port disabled by user command.	No action required.
Base port online: WWN = [Base Port WWN].	Information	Network and storage driver	2 (Port)	Online	Base port logged into fabric.	No action required.
Base port offline: WWN = [Base Port WWN].	Warning	Network and storage driver	2 (Port)	Offline	Base port logged out of fabric.	No action required.
Base port (WWN = [base port WWN or MAC]) lost fabric connectivity.	Error	Network and storage driver	2 (Port)	Logout	Base port lost connection with fabric.	Check switch and HBA configuration. Also, check SFP and cable connection stand-up adapters.
Heart Beat of IOC [IOC instance number] is good.	Information	Network and storage driver	9 (TOC)	Restart	Successful restart of firmware after a failure.	No action required.
Heart Beat of IOC [IOC instance number] has failed.	Critical	Network and storage driver	9 (TOC)	Crash	Firmware not responding.	Collect all error information and restart the firmware. Invoke bfa_supportsave.
IOC [IOC instance number] is enabled.	Information	Network and storage driver	9 (TOC)	Enabled	Adapter firmware started by user command.	No action required.
IOC [IOC instance number] is disabled.	Warning	Network and storage driver	9 (TOC)	Disabled	Adapter firmware stopped by user command.	No action required.
New adapter found: SN = [adapter serial number] base port WWN = [Base port WWN].	Information	Network and storage driver	1 (Adapter)	Added	Adapter added to host.	No action required.
New SFP found: port [base port number], Hardware Address = [Base port WWN or MAC]..	Information	Network and storage driver (stand-up adapters only)	2 (Port)	Found	User plugged in an SFP.	No action required.
QOS negotiation failed for base port: WWN = base port WWN or MAC].	Warning	Network and storage driver	2 (Port)	Failure	QoS negotiation failed.	Check switch and HBA configuration.

TABLE 13 Driver event messages (continued)

Message	Severity	Event Type	Category	Sub Category	Cause	Action
SFP removed: port [base port number], Hardware Address = [base port WWN or MAC].	Warning	Network and storage driver (stand-up adapters only)	2 (Port)	Removed	SFP removed.	Check if SFP is inserted properly.
SFP POM level to [aggregated SFP temperature, voltage, rx and tx power level]: port [base port number], Hardware Address = [base port WWN or MAC].	Warning	Network and storage driver (stand-up adapters only)	2 (Port)	Unhealthy	Change of current value against threshold of temperature, voltage and rx/tx power of SFP. Pluggable optical module (POM) plugs into the SFP.	If POM level is not normal, check the SFP.
Network Intermediate Driver Events						
VLAN id = # added/enabled on port mac = #	Information	Intermediate driver	VLAN		New VLAN created.	No action required.
New VLAN id = # removed/disabled from port mac = #.	Warning	Intermediate driver	VLAN		Existing VLAN deleted.	No action required.
New VLAN id = # added/enabled on mac = #	Information	Intermediate driver	VLAN	Team	New team VLAN created.	No action required.
New VLAN id = # removed/disabled from mac = #.	Warning	Intermediate driver	VLAN	Team	Existing team VLAN deleted.	No action required.
New team mac =# created/enabled.	Information	Intermediate driver	Team		New team created.	No action required.
Team mac = # deleted/disabled.	Warning	Intermediate driver	Team		Existing team deleted.	No action required.
A port is added to team mac = #.	Information	Intermediate driver	Team		An Ethernet port is added to an existing team.	No action required.
A port is removed from team mac = #.	Warning	Intermediate driver	Team		An Ethernet port is removed from an existing team	No action required.
Active port has changed in team mac = #	Information	Intermediate driver	Team		An ethernet port has become primary in the team.	No action required.

Appendix

HCM and Installer Message Reference

B

This appendix provides details on messages that display during operation of the Host Connectivity Manager (HCM) and Brocade Adapter Software Installer program. The following tables in this appendix provide reasons why these messages display and actions that you should take to resolve any problems associated with the messages:

- Table 14 provides details on messages that display during operation of the Host Connectivity Manager (HCM). Causes for each message and actions that you should perform are provided.
- Table 15 on page 137 provides details on messages that display during operation of the Brocade Adapter Software Installer program. Causes for each message and actions that you should perform are provided.

TABLE 14 Host Connectivity Manager messages

Message	Cause	Corrective Action or Notes
A maximum of eight ports are allowed in a team.	Occurs when the user tries to create a team with more than eight ports.	Create a team with eight or fewer ports.
A maximum of three IP addresses are allowed.	Occurs when more than three IP addresses are entered in the **Syslog Server Configuration** dialog box.	Configure three or less IP addresses.
Add Team failed. <Runtime Reason>	Occurs when addition of team failed due to runtime error.	• Refer to the runtime reason. • Refer to HCM logs. • Verify if the team was already added.
Add Team failed. Given adapter is part of another Team or VLANS exist.	Occurs when the user tries to create a team using an adapter for which are VLANs configured.	Do not create team when VLANs are configured.
After driver file upload, older agent is stopped.\nDriver update is started.	Older Agent stops after the driver upload.	Information message.
Add Team failed due to an unexpected error. <Runtime Reason>	Adding a team failed due to an unexpected error.	Determine why the error happens when adding a team.
All pending test(s) will be stopped. Started test(s) will continue to run until they are finished. Do you really want to close the window?	Occurs when the user stops a diagnostics test before it finishes.	Do not stop the test until it finishes.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
All statistics data displayed here will be lost if you do not save them. Do you want to proceed?	Occurs when the user closes the any **Statistics** dialog box.	Information message.
Are you sure you wish to clear the selected Name(s)?	Occurs when the user deletes the names in **Configure Names** using the **Remove** option.	Select **Yes** to delete the selected name and **no**, to not delete the selected name.
Authentication failed.	Occurs when adapter's authentication policy (CHAP secret, group, or algorithm) does not match with switch's authentication policy.	Enter the same authentication policy as the switch.
Backup data failed. <Runtime Reason>	Occurs when user tries to back up the data and the process of backup failed.	Error message. Backup failed in Runtime.
Backup data successfully completed.	Occurs when the data backup successfully completes.	Information message.
Backup of VLAN and Team configurations is successful.	Occurs when the user clicks on the **Backup VLAN and Team** menu item in **Tool** menu.	Information message.
Backup of VLAN and Team configurations is failed. <Runtime Reason>	Occurs when the user clicks on the **Backup VLAN and Team** menu item in **Tool** menu.	Error message. Backup failed in Runtime.
Backup is in progress. Please wait.	Occurs when the user initiates a backup operation using **HCM Backup** dialog box.	
Beaconing operation failed	Occurs in many cases. One case is if the user performs beaconing operation for a disabled port, the message "Port is not online Beaconing operation failed" displays.	Beacon port and beacon link for valid ports.
Boot image update is in progress. Do not close the dialog.	Occurs when user clicks the 'X' button in the **Update Boot Image** dialog box while the boot image update is in progress.	Information message.
Cannot connect to the server. Update failed.	Occurs when the user attempts operation in **Basic Port Configuration**, **Advanced Port Configuration**, or a **Reset** operation in a **Statistics** dialog box when the agent is not running.	Check if agent is still running.
Cannot get Teaming statistics for this host. No Teaming configured.	Occurs when the user launches the **Teaming Statistics** dialog box when there are no teams configured in the host.	Error message. Teams must be configured before using this dialog box.
Cannot find the adapter. Try again later.	Occurs when user enables or disables the adapter in the following scenario. 1 HCM discovers the adapter and places it into the product tree. 2 Another user removes the adapter before the next discovery. 3 User now tries to enable/disable the adapter.	Refresh the product tree and check if the adapter is still available.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
Choose any of the event severity levels to filter.	Occurs when the user selects an event severity level, and then clicks **OK** in the **Master Log Filter** dialog box.	Select at least one severity level (such as major or minor), and then click **OK** in the **Master Log Filter** dialog box.
Clear Filter cannot be performed while the Event Properties dialog is open.	Occurs if the **Event Properties** dialog is kept open and the user clicks **Clear Filter.**	Close the **Event Properties** dialog box, and then click **Clear Filter** to clear configured filters.
Could not validate the selected file as it does not have meta data information.\nAre you sure you want to continue?	Occurs when the meta data information is missing in the driver file.	Download a new driver and try again.
Dialog cannot be closed since the driver update\no-operation is in progress.	Occurs when the driver update or no-operation is in progress.	Information message.
Data Pattern for PCI Loopback Test cannot be empty. Enter valid data.	Occurs when the **Data Pattern** field is left empty while executing a PCI loopback Test.	Error message.
Data has been entered in preparation for adding a name but the name was not added. Do you want to add that name before you exit?	Occurs when user configures names in the following scenario. 1 Modifies name of any adapter or port 2 Enters WWN and name values in the **Detached WWN/MAC** and **Name** fields 3 Clicks **OK**.	Verify if the detached WWN/name is to be added to HCM alias store. If yes, click **Yes** to add or **No**.
Driver update is completed.	Occurs when the driver update has completed.	Information message.
Driver update is failed	Occurs when the driver update fails.	Information message.
Driver update is successful.	Occurs when the driver update is successful.	Information message.
Driver update is success. New agent {0} is up.	Occurs when the driver update is success and the new agent is running.	Information message.
Duplicate File: <Export File Name>. Do you want to replace the file?	Occurs when the user exports names to a file that already exists.	Try to export the names with a different file name.
Duplicate names still exists. Click cancel to discard duplicated names. Do you want to continue?	Occurs when the user selects **Cancel** button in **Duplicated Names** dialog box without making any changes.	Information message.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
Enter a valid host name or IP address	Occurs when the user clicks Add button in the **Syslog Server Configuration** dialog box without providing any host name or IP address or by providing an invalid host name or IP address.	Enter a valid host name and IP address in the host name field of the **Setup for Discovery** dialog box. Enter a valid host name/IP address in the Host name/IP address field of **Syslog Server Configuration** dialog box.
Enter a valid number for the test cycle.	Occurs when invalid number is provided in **Test Cycle** field.	Enter a valid number within the limit for the test cycle.
Event Filter cannot be launched while the Event Properties dialog is open.	Occurs when the user tries to launch the **Master Log Filter** dialog box while the **Event Properties** dialog box is open.	Close the **Event Properties** dialog box, and then launch the **Master Log Filter** dialog box.
Failed to connect to the Agent	Occurs when the agent connection is lost.	Start the HCM agent service, and then proceed.
Failed to create virtual port:	Occurs when there is a error while creating virtual ports.	Determine why the error happens when creating a virtual port.
Failed to refresh the team data due to an unexpected error. <Runtime Reason>	Occurs when an error occurs while refreshing the team data.	Determine why the error happens, and then proceed.
Failed to restore the VLAN and Team configurations. Reason: Caused by no saved configurations.	Occurs when there is VLAN/Teaming configuration file is not present to restore when user clicks **Tool** > **Restore Data** > **VLAN and Team**.	The VLAN and Teaming configuration save will only occur during installation or upgrade of network or intermediate drivers through the Brocade Adapters Software Installer (BASI). There must be a saved configuration for a successful restore.
Failed to restore the VLAN and Team configurations. <Runtime Reason>	Occurs when the restore of VLAN and Team configuration fails in HCM.	Retry the operation.
Fibre Channel Trunking cannot be enabled on the adapter {0} while QoS or TRL is enabled on the port {1}.	Quality of Service (QoS) or Target Rate Limiting (TRL) is enabled on an associated port.	Make sure QoS or TRL is disabled in any of the associated ports.
Found duplicate name(s). Please resolve.	Occurs when the user selects **User/Administrator will manually fix** option in the **Duplicated Name**s dialog box and does not provide a unique name.	Provide a unique name in the **Duplicated Name**s dialog box.
Frame Count for PCI Loopback Test cannot be empty. Enter valid data.	Occurs when the **Frame Count** field is left empty while executing a PCI loopback test.	Error message.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
Import of Names is complete, <Count> name(s) failed to import due to invalid WWW/MAC Address	Occurs when user imports the names file with invalid WWNs or MAC addresses.	Verify that all the WWNs and MAC addresses in the names file are valid.
Installation is not complete beyond the timeout value.\nClosing the driver update operation.	Occurs when the installation has not completed and the timeout value is reached.	Information message.
Invalid time range. Enter a valid time range.	Occurs when the user enters an invalid time range in the **Masterlog Log Filter** dialog box.	Enter a valid time range and collect the events logged for that time.
IOC for Port 1 will be disabled to enable trunking. Do you want to proceed?	Occurs when the user tries to enable trunking on the adapter.	Warning that selected port's IOC will be disabled when you enable trunking.
Log Invalid cannot be configured as Eth logging level.	Occurs when the user selects **Log Invalid** from the **Eth Logging Level** menu in the **Basic Port Configuration** dialog box.	Set valid logging level and proceed.
Log Invalid cannot be configured as Port logging level.	Occurs when the user selects **Log Invalid** from the **Port Logging Level** menu in the **Basic Port Configuration** dialog box.	Set valid logging level and proceed.
Loopback test cannot be performed on pre-boot disabled port	Occurs when user executes loopback test for preboot disabled port.	Make sure the preboot port is in enabled state and then execute the loopback test
Member not found. Team modification failed.	Occurs when user modified a team while another user removes the respective adapter.	Verify whether the adapter still exists in the host.
Modify Team failed due to an unexpected error. <Runtime Reason>	Occurs when a runtime error happens while modifying the team.	Determine why the error occurs.
Name should start with an alphabet. Allowed characters are 0-9, A-Z, a-z, hyphen (-) and underscore (_) and should not exceed 15 characters	Occurs when user provides a invalid name with special characters other than hyphen and underscore or name with more than 15 characters.	Enter a valid name which does not include any special character, other than hyphen and underscore, and is not more than 15 characters.
New password should not be blank.	Occurs when **New Password** field is left blank.	Enter a password in the **New Password** field and proceed
No configurations need to be saved	Occurs when the user selects **Apply** on the **VLAN Configuration** or **Teaming Configuration** dialog box without making any modifications.	Information message. Nothing was configured, so nothing will be saved.
No item found	Occurs when the user searches for a WWN/MAC/name that does not exist using the search option in the **Configure Names** dialog box.	Provide an existing WWN/MAC/name when searching.
No Team for deleting	Occurs when the user selects **Delete** when there is no team configured.	Information message.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
No tests have been selected. Select one or more tests.	Occurs when the user clicks **Start** without selecting any test.	Select a test, and then click **Start**.
Password cannot be blank.	Occurs when the **Password** field is left blank.	Enter a valid **Password** in the password field.
Password changed for agent.	Occurs when password is changed.	Information message.
Password has been successfully changed.	Occurs when password is changed successfully.	Information message.
Please assign at least one port for a Team	Occurs when the user clicks on **Apply** or **Ok** without selecting a port while creating or editing a Team configuration.	Be sure to selected a port when creating or editing a team.
Please select a Team	Occurs when the user selects **Statistics** or **Delete** without selecting a team.	Select at least one port while creating or editing a team.
Please select a VLAN	Occurs when the user selects Edit or Remove in the **VLAN Configuration** dialog box without selecting a VLAN.	Select a VLAN for editing or deleting in the dialog box.
Please type the same CHAP Secret.	Occurs when a different CHAP secret is entered in the **Retype Secret** field.	Enter the same CHAP secret in both the **CHAP Secret** and **Retype Secret** fields.
Please type a different password.	Occurs when user types in same value for old and new password fields.	Enter a different password other than old password.
Remove Team failed due to an unexpected error. <Runtime Reason>.	An unexpected error occur ed while removing a team.	Determine why the error happens when removing a team.
Port update failed for port. <Runtime reason>	Occurs when port configuration fails.	Verify if the agent is active.
Port <WWN> parameters update succeeded. Note: Setting will be enforced after port disable and enable.	Occurs when user makes configuration changes and clicks **Apply** to save the configurations.	Information message.
Provide a port number in the range [1025-65535].	Occurs when the user provides a port number out of the range (1025-65535) in the **Setup for Discovery** dialog box.	Enter a port number between 1025 and 65535.
QoS and Target rate limiting cannot be enabled at the same time.	Occurs when QOS and target rate limiting are enabled at the same time in the **Basic Port Configuration** dialog box.	Do not enable QOS and target rate limiting at the same time.
Refresh cannot be performed while the Event Properties dialog is open.	Occurs when the **Event Properties** dialog box is kept opened and the user tries to refresh the master log.	Close the **Event Properties** dialog box, and then click **Refresh** to display updated values.
Restore data is in progress. Please Wait.	Occurs when the user initiates a restore data operation using the **Restore data** dialog box.	Information message.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
Restore data is successfully completed. Please restart HCM for new data to take effect.	Occurs upon successful restore of backed-up HCM data.	Information message.
Select a valid driver file.	Occurs when driver file field is left blank.	Select the appropriate driver file.
Selected driver file version {0} is not supported.	Occurs when the selected driver version is not supported.	Use a supported driver.
Starting the driver update...	Occurs when the driver update starts.	Information message.
Successfully updated the parameters for all ports.	Occurs when the configurations done in the **Basic Port Configuration** dialog box are successfully updated using the **Apply** button.	The configuration will be reflected only after a successful process.
Syslog configuration failed	Occurs when the user tries to configure a syslog server using the **Syslog Server Configuration** dialog box.	Retry the operation.
System reboot is required for the newer driver to take effect	Occurs when the driver update is complete. A system reboot is required for the new driver to take effect.	Information message.
Team name should start with an alphabet. Allowed characters are 0-9, A-Z, a-z, hyphen (-) and underscore (_) and should not exceed 31 characters.	Occurs when the user provides an invalid team name.	Make sure the team name starts with a letter. Allowable characters in the team name are 0-9, A-Z, a-z, hyphen (-) and underscore (_).
The adapter will be disabled for executing the Memory test. This will also disable all the ports and their devices on the adapter. Are you sure you want to continue?	Occurs when the user selects the Memory test in the **Hardware Tests Diagnostics** dialog box.	Click **OK** to proceed or **Cancel** to cancel the operation.
The boot image update failed: <Runtime Reason>	Occurs when a invalid boot code image file is updated.	Select a valid boot image file for the boot image update.
The boot image successfully updated. You must reboot the system for the updated image to be effective.	Occurs when the boot code image is updated successfully.	After successful boot image update, reboot the system.
The change has not been sent to device. Do you want to commit the change?	Occurs when user clicks on OK in the **Basic Port Configuration** dialog box after making configuration changes.	Select to commit the change or to not commit the change.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
The changes will take effect only on port reset.	Occurs when the user adds a new authentication policy or edits the existing authentication policy in the **Fibre Channel Security Protocol** dialog box.	Information message.
The CHAP Secret and Retype Secret fields must have at least 8 alphanumeric characters.	Occurs when the secret key provided in the **CHAP Secret** and **Retype CHAP Secret** field is less than eight alphanumeric characters.	Provide a proper secret key which has at least 8 alpha numeric characters.
The External Loopback Test requires a plugged-in loopback cable; otherwise, the test will fail.	Occurs when the user selects external loop back test.	Plug in a loopback cable, and then run external loopback test to complete it successfully.
The file "{0}" does not exist	Occurs when file in the driver file field does not exist.	Select an existing driver file.
The following VLAN operation(s) failed: <VLAN operation>:<Runtime Reason>	An error occurs while creating or deleting a VLAN.	Determine the problem with creating or deleting a VLAN, and then proceed.
The Name is already in use. Enter a different name or clear the existing name.	Occurs when the user enters duplicate name in **Configure Names** or **Define Names** dialog box.	Provide unique names in these dialog boxes.
The operation will take effect after you click OK or Apply on the Configuration dialog.	Occurs when the user makes configuration changes in the **Basic Port Configuration** dialog box and clicks **Apply** or **OK**.	Clicking **Apply** or **OK** will make the configuration changes.
The specified file is not a valid file to import.	Occurs when invalid file is imported through the **Configure Names** dialog box.	Import a valid file with appropriate data in the **Configure Names** dialog box.
The team name is duplicated. Please enter a qualified Team Name.	Occurs when the user tries to add a team with existing team name.	Provide different name for the new team.
The virtual node WWN is not valid. Enter a valid Node WWN.	Occurs when the user enters a invalid WWN in the **Virtual Port Creation** dialog box.	Provide valid WWN.
The virtual port is a duplicate. Enter a valid WWN.	Occurs when the user enters a duplicate virtual port WWN in the **Virtual Port Creation** dialog box.	Provide a unique virtual port WWN.
The VLAN name is reserved. Please choose a different one.	Occurs when the name provided for a VLAN is already reserved.	Use a unique name for the VLAN.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
The WWN or MAC address already exists in the All WWNs/MACs table. Edit the existing record(s). Record(s) with the same WWN address are highlighted.	Occurs when user enters a WWN or MAC address which is already present the **WWN/MAC** field in the **Devine Names** dialog box.	Check the same WWN or MAC address is available in the WWNs/MAC view of the **Configure Names** dialog box. Enter a different WWN or MAC address.
There are VLANs associated with the port you have selected to be added as a member of the team. If you add the port, all associated VLANS will be removed. Are you sure you want to add this port to the team and remove all associated VLANs?	Occurs when the user creates a team with a port for which a VLAN is already configured.	Remove the VLAN configured for the port, and then try creating a team with that port.
This action resets all listed counters. Do you want to continue?	Occurs when the user selects **Reset** on a **Statistics** dialog box.	Select **Yes** to reset all the counter values in the dialog box.
Unexpected Error. Test(s) will be stopped.	Occurs when the user tries to execute the diagnostics test when the agent is stopped.	Start the agent, and then execute the diagnostics test.
Unexpected Error. eth Loopback Test will be stopped. Please contact the technical support	Occurs when the user executes the loopback test for a port and connection is lost.	Verify the connection, and then proceed with loopback test.
Unable to find the host. Please provide another host.	Occurs when an invalid host name or IP address is given in **Host Name** field in the **Setup for Discovery** dialog box.	Enter a valid host name or IP address in the **Host Name** field.
Unable to extract the driver file {0}.	Occurs when the driver cannot be extracted.	
Unable to find the host. Please provide another host.	Occurs when link local ipv6 address (such as fe80:216:cbff:fea9:c3b5%en0 or fe80:216:cbff:fea9:c3b5%3) is provided in the **Setup for Discovery** dialog box.	Provide the IPv6 address without using the scope-id and the delimiter (%). Just use fe80:216:cbff:fea9:c3b5.
Unable to retrieve the driver update status.	Occurs when the driver update status cannot be retrieved.	Information message.
Update is not started beyond the timeout value. Closing the driver update operation.	Occurs when the driver update did not start the timeout value was reached.	Information message.
Uploading of the driver file is failed.	Occurs when driver file upload failed to Agent host.	Information message.
Uploading of the driver file is failed. Reason - Maintenance mode is not enabled or could not be determined.	ESX systems must be in maintenance mode to update drivers.	Place system in maintenance mode and reinstall driver(s).

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
Uploading the driver file to the agent {0}	Occurs when HCM GUI uploads the driver file to the agent.	Information message.
Uploading the driver file is successful.	Occurs when driver file uploaded successfully to the Agent host.	Information message.
VLAN and Team configurations successfully restored.	Occurs when the VLAN and Team configurations are successfully restored in HCM.	Information message.
<WWN> is an invalid WWN or MAC	Occurs when the user adds a invalid WWN (for example, 00:00:00:00:00:00:00:00) or invalid MAC address (for example, 00:00:00:00:00:00) in the **Detached WWN/MAC** field or **Configure Names** dialog box.	Add a valid WWN or MAC address in the **Detached WWN/MAC** field or **Configure Names** dialog box. Provide a valid MAC address in the **Detached WWN/MAC** field.
You are going to stop the pending test(s) only. All Started test(s) will continue to run. Are you sure you want to continue?	This occurs when the user stops a diagnostics test before it finishes.	Information message.
You are about to delete a large number of virtual port(s). Are you sure you want to continue?	Occurs when user deletes virtual ports the **Virtual Port Deletion** dialog box were configured using HCM and BCU.	Information message.
You are about to delete all the test logs. Are you sure you want to continue?	Occurs when the user selects a test log and selects option to clear the log.	Warning. This clears all the test logs.
You are about to disable the Port <WWN>. This will disable all the devices on this Port. Are you sure you want to continue?	Occurs when port is disabled from the right-click drop down menu for the port and in the **Basic Port Configuration** dialog box.	Warning that disabling the port will disable all the devices on the port. Confirm that you wish to do this.
You are about to send the information to the agent. Do you want to proceed?	Occurs when the user performs actions in the **Configure Names** dialog box and selects **OK** or **Apply.**	Either select **Yes** to save all configurations or **No** to discard configurations.
You are about to update boot image to all Adapters. Are you sure you want to continue?	Occurs when the user clicks OK to update the boot code image for all installed adapters.	Information message.
You did not select any virtual port. Select one or more virtual ports.	Occurs when the user selects **Apply** on the **Virtual Port Deletion** dialog box without selecting any virtual ports.	Select the desired virtual ports, then select **Apply**.

TABLE 14 Host Connectivity Manager messages (continued)

Message	Cause	Corrective Action or Notes
You do not have write permission to export file to the folder <path>	Occurs when user tries to export a names file to a folder where access is denied.	Make sure the folder has write permission and then export names file to that folder.
You have unsaved configurations. Do you want to save the previous configurations?	Occurs when the user removes, adds, or edits VLANS in the **VLAN Configuration** dialog box, and then clicks **Cancel**.	Either select **Yes** to save the unsaved configurations or **No** to not save the unsaved configurations.

Table 15 provides details on messages that display during operation of the Brocade Adapter Software Installer program. Causes for each message and actions that you should perform are provided.

TABLE 15 Brocade Adapter Software Installer messages

Message	Cause	Corrective Action or Notes
A newer version of the product <VERSION> is already installed in this system. Downgrading to an older version is not allowed. Installer will quit now. Please refer to the Installation and Reference manual for the recommended downgrade procedure.	Occurs when there is a new version of the software installed already in the system and you try to downgrade with an older version.	The installer quits the installation. Install the latest software for the installed adapter.
Could not proceed with the Installation of driver as the below Hot Fixes are missing <HOT FIX MISSING INFO> Please download the Hot Fix from the below website and retry installation of driver http://www.microsoft.com/downloads/en/default.aspx	Occurs when a hot fix is missing in Windows systems.	Download the hot fix from http://www.microsoft.com/downloads/en/default.aspx website, install the hot fix, and then try installing the software.
Default module loading setting The Driver module was not loaded because of the variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" in /etc/sysconfig/hardware/config file is set to “no”, please change it to “yes” and retry the installation.	Occurs when the variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" in /etc/sysconfig/hardware/config file is set to “no”.	Change the “No” to “Yes” in variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" located in /etc/sysconfig/hardware/config file then proceed with installation.
Default module loading setting The Driver module was not loaded because of the Variable "allow_unsupported_modules" in /etc/modprobe.d/unsupported-modules file is set to “0”, please change it to “1” and retry the installation.	Occurs when the variable "allow_unsupported_modules" in /etc/modprobe.d/unsupported-modules file is set to “0”	Change the “0” to “1” in variable "allow_unsupported_modules" located in /etc/modprobe.d/unsupported-modules file then proceed with installation.
Default module loading setting Variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" in /etc/sysconfig/hardware/config file is set to “no”, please change it to “yes” before continuing installation otherwise the driver module will not be loaded.	Occurs when the variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" in the /etc/sysconfig/hardware/config file is set to “no”.	Change the “No” to “Yes” in variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" in /etc/sysconfig/hardware/config file then continue installation.

TABLE 15 Brocade Adapter Software Installer messages (continued)

Message	Cause	Corrective Action or Notes
Disk space calculation Available space is <Available space>. Please free up at least 50 MB in /opt and re-attempt the installation.	Occurs when the available space in /opt is less than 50MB.	Free at least 50MB in /opt, and then try installation.
Do you want to back up the HCM configurations? Configurations are stored in data directory. <Three buttons displays like Don't Backup, Backup and Cancel>	Occurs when you remove the application.	If you want to back up the data, click on "Backup" or else click "Don't backup."
File backup Successfully backed up <brcd_initrd_backup_filename> in /boot.	Occurs when Initrd file is backedup successfully in /boot.	No action required.
File backup There is a back up file <brcd_initrd_backup_filename> already available in /boot. Do you want to overwrite?	Occurs when a backup file named <brcd_initrd_backup_file name> is already available in /boot	When user wish to overwrite the existing backup file press "Yes" else "No"
Found Backed up data. Backed up configuration directory of HCM <backedup_gui_version> dated <Backup_Date> is found at <Backup_Directory>. Do you want to restore old configurations?	Occurs during the course of installation when a backup data is already present in the system.	If the user wishes to restore the backed-up data, the user can give "Yes" else "No"
No matching binary rpm found Do you want to install noarch rpm? Note: - noarch rpm is not recommended for RHEL/SLES. - noarch rpm requires kernel devel/source rpm and GCC.	Occurs when a matching binary rpm is not found.	Click **Yes** to proceed with the installation using the noarch rpm or click **No** to stop installation.
Path is not Valid. You have entered an invalid backup output directory. Please make sure the directory path is correct.	Occurs if provide an invalid path name or leave the **path** field blank.	Enter a valid path to backup the files.
Pre-Installation Message It is strongly recommended that you quit all HCM application running on this machine before continuing with the Upgrade/Reinstall.	Occurs after the upgrade/reinstall message.	Stop HCM from running before upgrading or reinstalling the software.
Pre-requisite check is done...	Occurs when driver's pre-requisite check is completed.	Information message.
Pre-Uninstallation Message It is strongly recommended that you quit all HCM application running on this machine before continuing with the Upgrade/Reinstall.	Occurs during removing the HCM application.	Close HCM or the installer will close it before proceeding with software removal.

TABLE 15 Brocade Adapter Software Installer messages (continued)

Message	Cause	Corrective Action or Notes
Please free up at least 50MB in the /opt directory and try the installation again.	Occurs when the space in the /opt directory is less than 50MB.	Free at least 50MB and then proceed with installation.
Please note that your system is Windows 2003 x86 Service Pack 1. There is no brocade adapter driver available for Windows 2003Service Pack 1. Please get Service Pack 2 from: http://www.microsoft.com/downloads/details.aspx?FamilyID=95ac1610-c232-4644-b828-c55eec605d55&displaylang=en	Occurs when you install the driver on a Windows 2003 x86 SP1 system.	Upgrade SP1 to SP2, and then try installing the driver.
Please note that your system is Windows 2003 x64 Service Pack 1. There is no brocade adapter driver available for Windows 2003Service Pack 1. Please get Service Pack 2 from: http://www.microsoft.com/downloads/details.aspx?FamilyID=95ac1610-c232-4644-b828-c55eec605d55&displaylang=en	Occurs when you install the driver on a Windows 2003 x64 SP1 system.	Upgrade SP1 to SP2, and then try installing the driver.
ReStart Message For Solaris SUCCESSFUL installation of Driver may require System	Occurs in all Solaris systems when the driver is installed successfully.	Restart the system to complete installation.
ReStart Message For Linux Please reboot your system for the new driver to get loaded.	Occurs when the driver is installed successfully on Linux systems.	Restart the system to complete installation.
ReStart Message For Solaris SUCCESSFUL uninstallation of driver may require System	Occurs for Solaris systems when the driver is successfully removed.	Restart the system to complete removal.
ReStart Message For Linux SUCCESSFUL uninstallation of driver may require System	Occurs on Linux systems when the driver is successfully removed.	Restart the system to complete removal.
System dependencies not available. GCC and Kernel rpms are required for installing Storage and Network Driver and HCM and Storage and Network Driver. Variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" in /etc/sysconfig/hardware/config file is set to “no”, please change it to “yes” before continuing installation otherwise the driver module will not be loaded.	Occurs when you install a drivers on a Linux system that does not contain GCC and Kernel rpm and when the variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" in /etc/sysconfig/hardware/config file is set to “no”.	Change the “No” in variable "LOAD_UNSUPPORTED_MODULES_AUTOMATICALLY" present in /etc/sysconfig/hardware/config file to “Yes.” Load the GCC and Kernel rpms onto the system and install the drivers.

TABLE 15 Brocade Adapter Software Installer messages (continued)

Message	Cause	Corrective Action or Notes
System dependencies not available. GCC and Kernel rpms are required for installing Storage and Network Driver and HCM and Storage and Network Driver. Variable "allow_unsupported_modules" in /etc/modprobe.d/unsupported-modules file is set to “0”, please change it to “1” before continuing installation otherwise the driver module will not be loaded.	Occurs when you install drivers on a Linux system that does not contain the GCC and kernel rpm and when the variable "allow_unsupported_modules" in /etc/modprobe.d/unsupported-modules file is set to “0”	Change the “0” in variable "allow_unsupported_modules" present in /etc/modprobe.d/unsupported-modules file to “1.” Load the GCC and Kernel rpms on the system, and install the drivers.
System dependencies not available. GCC and Kernel rpms are required for installing Storage and Network Driver and HCM and Storage and Network Driver.	Occurs when you install drivers on Linux systems that do not contain the GCC and Kernel rpm.	Load the GCC and kernel rpms on the system and then install the drivers.
The following component(s) exist in your system. Product : <Already installed version> <Components list displays with tabular format> HCM/ configuration preference - option 1 -> Install with existing configuration - option 2 -> Install with default configuration <Two buttons displays like Continue, Exit>	Occurs when you try to overwrite currently installed software with a newer version.	Select whether you want to install software using the default configuration or the configuration that exists for the currently installed software.
The following component(s) exist in your system. Product : <Installer Driver Name> <Components list displays with tabular format> <Two buttons displays like Continue and Exit >	Occurs when a driver was installed using native installer scripts or system commands and you are trying to overwrite with a newer driver.	Continue installing new components or exit the installation.
Unable to start the driver update.	Occurs when driver update not able to start.	Information message.
VLAN ID cannot be empty. Enter a valid VLAN ID.	Occurs when the user add a new VLAN without providing a VLAN ID in the **VLAN Configuration** dialog box.	Provide a valid VLAN ID while creating VLAN.
Warning message If booting over Brocade HBA, you must have a version of driver installed before you restart the system.	Occurs on Linux systems during removal of driver or HCM and driver.	If booting a Brocade HBA, make sure driver is installed in the system before rebooting.
Would you like to overwrite the existing driver? The adapters on the system have a better driver version than the one you are trying to install. Click OK to continue.	Occurs when the system has a better driver version than the one you are installing.	If you want to overwrite the existing driver, click OK to continue.

Index

A

adapter
- diagnostics, *89*
- event message files, *68*
- hardware supported, *xii*
- IP address lost, *33*
- list command, *111*
- queries, *111*
- query command, *111*
- software supported, *xii*
- statistics, *73*

adapter BIOS messages, *121*
adapter management, BCU, *65*
adapter not registering with name server, *42*
adapter not reported under PCI subsystem, *9*
adapter not showing in fabric, *41*
adapter properties, *109*
application log, *70*, *71*
applications using TDI driver stop responding, *36*
authentication settings, *105*
authentication statistics, *73*
- displaying through BCU, *74*
- displaying through HCM, *74*

B

BCU command problems, *14*
BCU commands
- adapter list, *111*
- adapter query, *111*
- port list, *103*
- port query, *103*
- port speed, *103*
- team --list, *105*
- team --query, *105*
- to collect data, *61*
- using for ESX systems, *66*

BCU commands, using, *65*
BCU desktop shortcut missing problem, *16*
BCU version mismatch, *14*
beaconing, *89*
- enabling through BCU, *89*
- enabling through HCM, *90*

binding issues with Hyper-V enabled, *39*
BIOS data through BCU, *97*
BIOS data, collecting, *97*
BIOS messages, *121*
BIOS not installed displays, *27*
bios query command, *97*
boot from SAN stops on HP hosts, *26*

C

cannot boot over SAN, *26*
cannot disable trunking, *30*
cannot manage CNAs after attempting upgrade, *31*
cannot remove Linux driver, *17*
CNA
- fabric OS support, *xiii*
- host support, *xiv*
- problems, *31*
- storage support, *xiii*
- supported models, *xii*
- switch support, *xiii*

CNA MAC addressing, *xxii*
CNA operating system support, *xiv*
collecting data
- using event logs, *69*
- using Fabric OS commands, *66*

CTL-B option does not display when booting host, *24*

D

data
- collecting with BCU and HCM, *61*
- collecting with host commands, *59*

data to provide support, *58*
DCB is not enabled, *45*
DCB links, verifying, *50*
DCB network problems, *45*

DCB port performance statistics, *83*
DCB statistics, *74*
device drivers not loading, *18*
device drivers not loading in Windows problem, *11*
device manager, *52*
diagnostics
adapter, *89*
beaconing, *89*
enabling through BCU, *89*
enabling through HCM, *90*
echo test
enabling through BCU, *96*
enabling through HCM, *96*
Ethernet loopback tests
enabling through HCM, *91*
HBA temperature, *94*
loopback tests, *90*
enabling through BCU, *90*
enabling through HCM, *91*, *94*
memory test, *93*
enabling through BCU, *93*
enabling through HCM, *93*
PCI loopback tests, *92*
enabling through BCU, *92*
enabling through HCM, *92*
ping end points, *93*
enable through HCM, *94*
enabling through BCU, *93*
predictive optical monitoring, *98*
queue test, *94*
SCSI test, *95*
SFP enable through BCU, *98*
trace route, *95*
enable through HCM, *95*
enabling through BCU, *95*
driver and operating system install failure, *23*
driver event messages, *13*, *122*
driver incompatible with CNA drivers, *16*
driver install errors, *19*
driver installation fails, *17*
driver installation fails on ESX systems, *19*
driver package
confirming installation, *52*
confirming Linux installation, *53*
confirming Solaris installation, *54*
confirming VMware installation, *54*
confirming Windows installation, *52*
driver preinstallation, *23*
driver tunable parameters for Windows, *115*

E

echo test, *96*
enable through HCM, *96*
enabling through BCU, *96*
enable and disable VLANs in Device Manager, *38*
errors when installing driver package, *19*
errors when using GUI software installer, *19*
ESX systems BCU commands, *66*
Ethernet, *68*
Ethernet link ports or LOM not coming up, *33*
Ethernet loopback test problems, *32*
Ethernet loopback tests
enabling through HCM, *91*
Ethernet port properties, *100*
event logging levels, *71*
event logs, *69*
HCM, *70*
host system, *69*
syslog support, *69*
Windows event log support, *69*
event message files, *68*
event message reference, *127*

F

Fabric Adapter problems, *27*
fabric authentication failures, *41*
Fabric OS commands, *66*
fabric statistics, *76*
displaying through BCU, *76*
displaying through HCM, *77*
failed to connect to agent on host error, *46*
FC port properties, *101*
FCoE and Fibre Channel, *41*
FCoE link is down, *43*
FCoE port properties, *100*
FCoE statistics, *75*
FCP IM module statistics, *77*
FCP initiator mode statistics, *77*
FCP-IM I/O profiling, *104*
Fibre Channel Association, *xxi*
Fibre Channel links, verifying, *50*
files needed for bfad.sys message, *18*

G

graphs, *81*
graphs on performance, *81*

H

HBA
    PWWN, *xxii*
    serial number, *xxii*
    supported models, *xiii*
HBA and CNA problems, *9*
HBA memory test, *93*
HBA problems, *28*
HCM Agent not auto starting, *49*
HCM logging levels, *72*
HCM logs, *70*
HCM not discovering all Ethernet ports for vNICs, *28*
HCM not discovering ports for vNICs, *28*
HCM options to collect data, *61*
HCM time doesn't match system, *50*
host commands for collecting data, *59*
host freezes or crashes, *12*
host not booting from remote LUN, *20*
host operating system support
    adapter drivers, *xiv*
    HCM, *xvi*
host system freezes, *12*
host system logs, *69*
host system with adapter fails to hibernate, *16*

I

I/O data traffic issues, *15*
I/O performance statistics, *79*
I/O problem on FCoE device, *44*
I/Os not failing over on path failure, *44*
information gathering for troubleshooting, *3*
installation
    confirming driver installation, *52*
    confirming driver package, *52*
    confirming driver package in Linux, *53*
    confirming driver package in Solaris, *54*
    confirming driver package in VMware, *54*
    confirming driver package in Windows, *52*
    driver errors, *19*
    verifying for drivers, *51*
installation failure on boot, *22*
installing Windows DUD results in offline disk, *23*

L

Linux network driver tuning, *117*
Linux storage driver tuning, *113*
LLDP data, collecting, *97*
log
    application, *70*
    master, *70*
logging levels, adjusting, *71*
logical port properties, *102*
logical port statistics, *80*
    displaying through BCU, *81*
    displaying through HCM, *80*
logs
    adjust logging level, *71*
    application, *71*
    event, *69*
    HCM, *70*
    host system, *69*
    master log severity levels, *70*
    port, *102*
    syslog support, *69*
loopback tests, *90*
    enabling through BCU, *90*
    enabling through HCM, *91*, *94*
loss of adapter hardware address, *33*
loss of synch and signal errors, *41*
low throughput and high latency on Linux, *45*
LUN not visible, *25*

M

MAC addressing, *xxii*
master log, *70*
master log severity levels, *70*
memory test, *93*
    enabling through BCU, *93*
    enabling through HCM, *93*
message reference, *122*, *127*
messages
    BIOS, *121*
    driver event, *122*

N

network interface problems for CNAs and NICs, *32*
network stack runs out of heap, *34*
NIC numbering on VMware unexpected, *34*
no adapters found on local host, *28*
no adapters reported, *10*
no target devices found or link down message, *25*

O

one adapter port participates in trunk, *29*
operating system errors, *13*
operating system support
    CNA, *xiv*
    Ethernet, *xv*
    FCoE, *xv*
    Fibre Channel, *xiv*
    Hypervisor, *xvi*

P

PCI loopback tests, *92*
    enabling through BCU, *92*
    enabling through HCM, *92*
pcifn and vhba commands return errors problem, *14*
performance, *81*
    data, *81*
    port, *82*
performance optimization
    Linux network driver tuning, *117*
    Linux storage driver tuning, *113*
    Solaris network driver tuning, *119*
    Solaris storage driver tuning, *114*
    VMware network driver tuning, *117*
    VMware tuning, *116*
    Windows network driver tuning, *116*
    Windows storage driver tuning, *114*
performance statistic, *83*
persistent binding settings, *108*
PHY module data, *81*, *106*
ping end points diagnostics, *93*
    enable through HCM, *94*
    enabling through BCU, *93*
ping to server failing, *34*
POM field, *98*
poor network performance, *39*
port data, *99*
port link not up, *10*
port list command, *103*
port log, *102*
port logging levels, *71*
port performance statistics through BCU, *82*
port properties
    base, *99*
    logical, *102*
    remote, *101*
    virtual, *102*
port properties panel, *99*
port query command, *103*
port speed command, *103*
port statistics, *82*
    enable through BCU, *83*
    enable through HCM, *83*

problem
adapter loses IP address, *33*
adapter not registering with name server, *42*
adapter not reported under PCI subsystem, *9*
adapter not showing in fabric, *41*
applications using TDI driver stop responding, *36*
BCU shortcut missing, *16*
BCU version mismatch, *14*
binding issues with Hyper-V enabled, *39*
BIOS not installed displays, *27*
boot from SAN stops on HP hosts, *26*
cannot boot over SAN, *26*
cannot disable trunking, *30*
cannot manage CNAs after attempting upgrade, *31*
cannot remove Linux driver, *17*
CNA, *31*
CTL-B option does not display when booting host, *24*
DCB network, *45*
DCB not enabled, *45*
device drivers not loading, *18*
devices drivers not loading in Windows, *11*
driver event messages in host logs, *13*
driver incompatible with CNA driver, *16*
driver installation fails, *17*
driver installation fails on ESX systems, *19*
driver preinstallation, *23*
errors when installing Linux driver, *19*
errors when using GUI software installer, *19*
Ethernet link ports or LOM not coming up, *33*
Ethernet loopback test problems, *32*
Fabric Adapter, *27*
fabric authentication failures, *41*
failed to connect to agent on host error, *46*
FCoE and Fibre Channel, *41*
FCoE link is down, *43*
files needed for bfad.sys message, *18*
HCM Agent not auto starting, *49*
HCM not discovering all Ethernet ports for vNICs, *28*
HCM not discovering ports for vNICs, *28*
host not booting from remote LUN, *20, 21*
host system freezes, *12*
host system with adapter fails to hibernate, *16*
I/O data traffic issues, *15*
I/O problem on FCoE device, *44*
I/Os not failing over on path failure, *44*
installation failure on boot LUN, *22, 23*
loss of adapter hardware address, *33*
loss of sync and signal errors, *41*
low throughput and high latency, *45*
low throughput and high latency on Linux, *45*
low throughput and high latency on VMware, *45*
LUN not visible, *25*
network interface (CNA for NIC), *32*
network stack runs out of heap, *34*
NIC numbering on VMware unexpected, *34*
no adapters found on local host, *28*
no adapters reported, *10*
no target devices found or link down, *25*
offline disk occurs after installing Windows DUD, *23*
only one adapter port participates in trunk, *29*
operating system errors, *13*
pcifn and vhba commands return errors, *14*
ping to server failing, *34*
poor network performance, *39*
port link not up, *10*
QoS performance issues, *28*
quality of service not functioning, *29*
receive-side scaling disables, *35*
removing network drivers causes error, *17*
resolving BIOS boot problems, *23*
resolving UEFI boot problems, *20*
RSS network throughput decreasing, *36*
SNMP browser not displaying all information, *36*
software installer does not autorun, *12*
system not booting over SAN or local disk in legacy BIOS, *20*
target not visible from remote host, *24*
teaming errors, *36*
teaming or VLAN operations fail through HCM, *38*
time in HCM does not match system, *50*
trunked port disables on switch, *30*
trunking, *29*
unable to boot from device, *25*
unable to create NPIV ports, *30*
unable to uninstall HCM, *49*
virtual devices not listed in name server, *42*
VLAN creation and operation, *37*
VLANS and teams persist after changing port to HBA mode, *27*
VMQs not created, *31*
problem information, *3*
problems using BCU commands, *14*
product information resources, *xx*
profiling FCP-IM I/O tool, *104*
profiling for FCP initiator mode statistics
BCU, *77*
properties
adapter, *109*
Ethernet port, *100*
FC port, *101*
FCoE port, *100*
vHBA, *101*
properties for SFPs, *98*
publication references, *56*

Q

QoS performance issues, *28*
QoS statistics, *85*
    displaying through BCU, *85*
    displaying through HCM, *85*
quality of service (QoS), *106*
quality of service not functioning, *29*

R

receive-side scaling (RSS) disables, *35*
references for isolating problems, *56*
remote port properties, *101*
remote port statistics, *84*
    displaying through BCU, *85*
    displaying through HCM, *84*
resolving BIOS boot problems, *23*
resources for product information, *xx*
RSS network throughput decreasing, *36*

S

SCSI target ID mappings, *108*
serial number location, *xxii*
SFP attributes, monitoring, *98*
SFP diagnostics enable through BCU, *98*
SFP diagnostics enable through HCM, *98*
SFP properties, *98*
SNMP browser not displaying all information, *36*
software installer does not autorun, *12*
Solaris network driver tuning, *119*
Solaris storage driver tuning, *114*
statistics
    authentication, *73*
        displaying through BCU, *74*
        displaying through HCM, *74*
    DCB, *74*
        displaying through BCU, *75*
        displaying through HCM, *75*
    fabric, *76*
        displaying through BCU, *76*
        displaying through HCM, *77*
    FCoE, *75*
    FCP IM module, *77*
        displaying through HCM, *77*
    FCP initiator mode, *77*
    firmware, *78*
    logical port, *80*
        displaying through BCU, *81*
        displaying through HCM, *80*
    performance, *83*
    PHY module, *81*
    port, *82*
        display through BCU, *83*
        display through HCM, *83*
    QoS
        displaying through BCU, *85*
        displaying through HCM, *85*
    remote port, *84*
        displaying through BCU, *85*
        displaying through HCM, *84*
    vHBA, *86*
        displaying through BCU, *86*, *87*
        displaying through HCM, *86*
    virtual port, *87*
        displaying through BCU, *88*
        displaying through HCM, *88*
    VLAN for ports, *89*
    VLAN for teams, *88*
        displaying through BCU, *88*
        displaying through HCM, *88*
    vNIC, *86*
        displaying through HCM, *87*
statistics for adapters, *73*
storage driver tunable parameters for Windows, *114*
storage driver tuning, *113*
support data to provide, *58*

support save
differences between HCM, BCU, and browser, *65*
using, *61*
using BCU on ESX systems, *64*
using HCM, *63*
using Management applications, *63*
using through BCU, *64*
using through browser, *64*
using through port crash event, *65*
syslog support, *69*
system not booting over SAN or local disk in Legacy BIOS, *20*

T

target not visible from remote host, *24*
target rate limiting settings, *107*
target statistics, *84*
team --list command, *105*
team --query command, *105*
teaming configuration dialog box, *104*
teaming errors, *36*
teaming information, *104*
teaming or VLAN operations fail through HCM, *38*
technical help for product, *xxi*
temperature diagnostics, *94*
time on HCM doesn't match system, *50*
trace route, *95*
enable through HCM, *95*
enabling through BCU, *95*
trunked port disables on switch, *30*
trunking attributes, displaying, *85*
trunking problems, *29*

U

UEFI boot, *20*
UEFI boot problems, *20*
UEFI data, collecting, *97*
unable to boot from device, *25*
unable to create NPIV ports, *30*
unable to uninstall HCM, *49*

V

verifying driver installation, *51*
verifying Fibre Channel and DCB links, *50*
vHBA properties, *101*
vHBA statistics, *86*
displaying through BCU, *86, 87*
displaying through HCM, *86*
virtual devices not listed in name server, *42*
virtual port properties, *102*
virtual port statistics, *87*
displaying through BCU, *88*
displaying through HCM, *88*
VLAN creation and operation problems, *37*
VLAN statistics for a team, *88*
VLANs and teams persist after changing port mode, *27*
VLANs enable and disable in Device Manager, *38*
VMQs not created, *31*
VMware network driver tuning, *117*
VMware tuning, *116*
vNIC statistics, *86*
displaying through HCM, *87*

W

Windows network driver tuning, *116*
Windows problem
files needed for bfad.sys message, *18*
installer program does not autorun, *12*
Windows storage driver tunable parameters, *114*
Windows storage driver tuning, *114*
WWPN of HBA, *xxii*